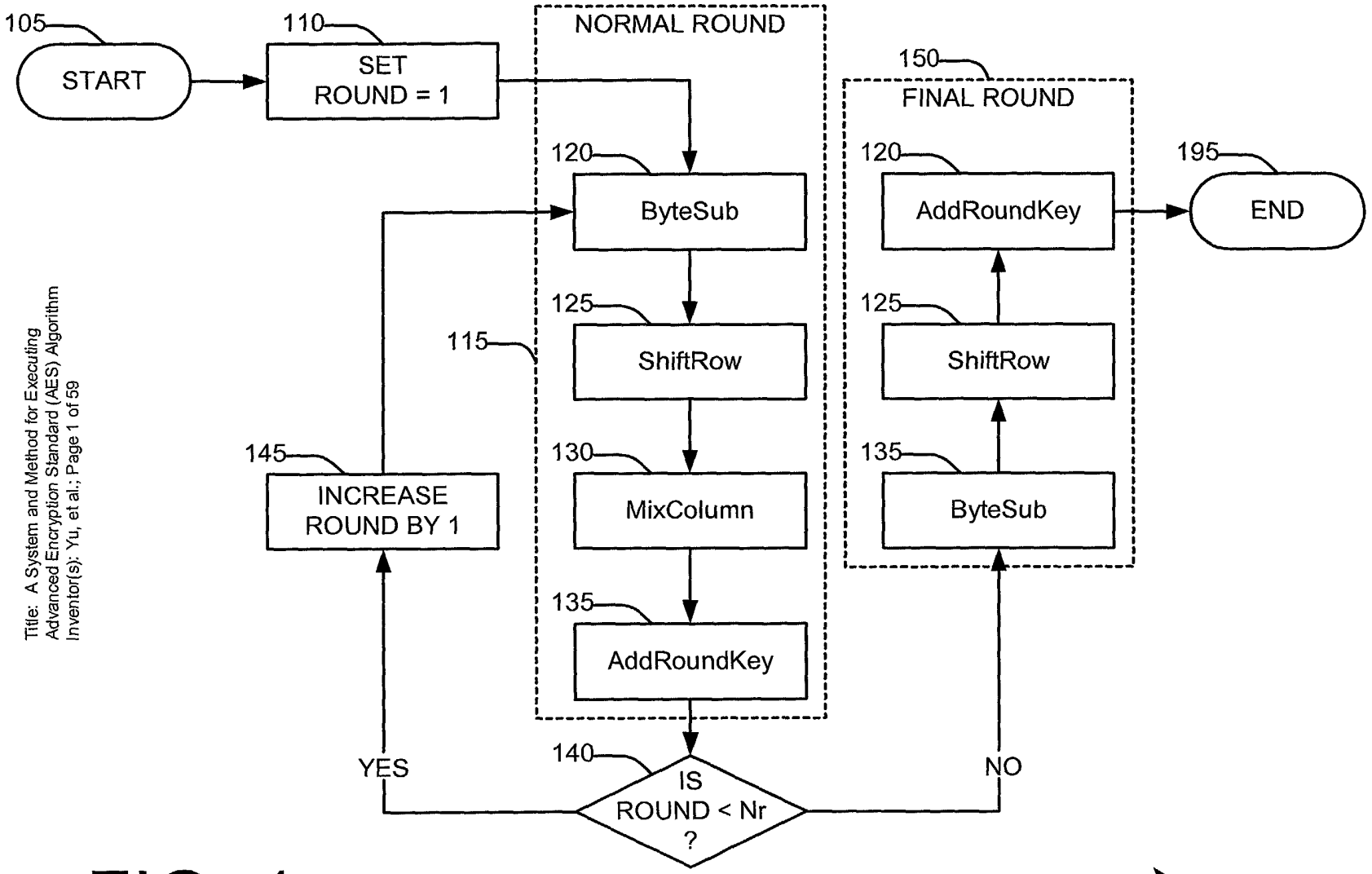
20020 0798901



Title: A System and Method for Executing
Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 1 of 59

FIG. 1
(PRIOR ART)

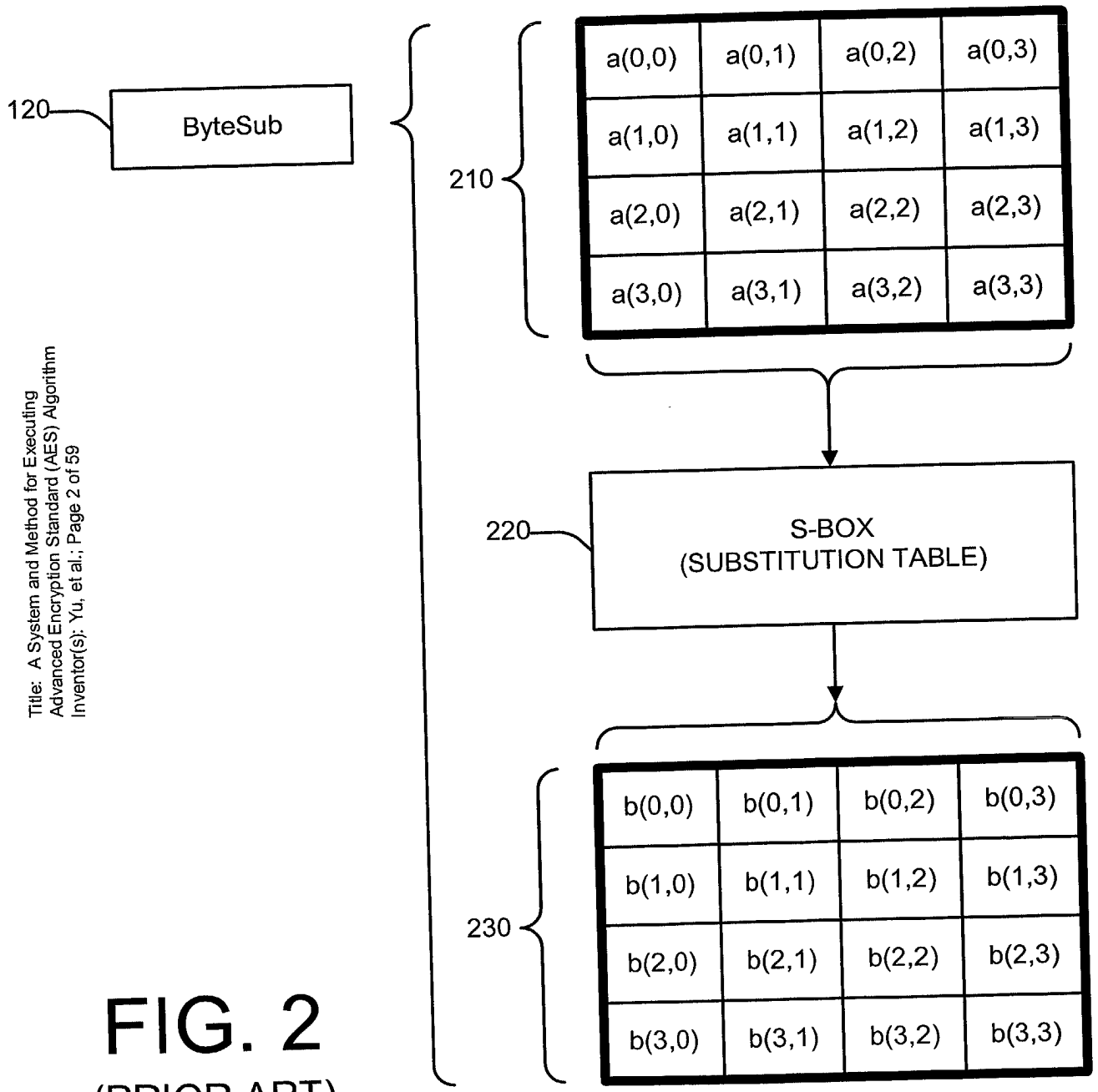


FIG. 2
(PRIOR ART)

20020" 0198901

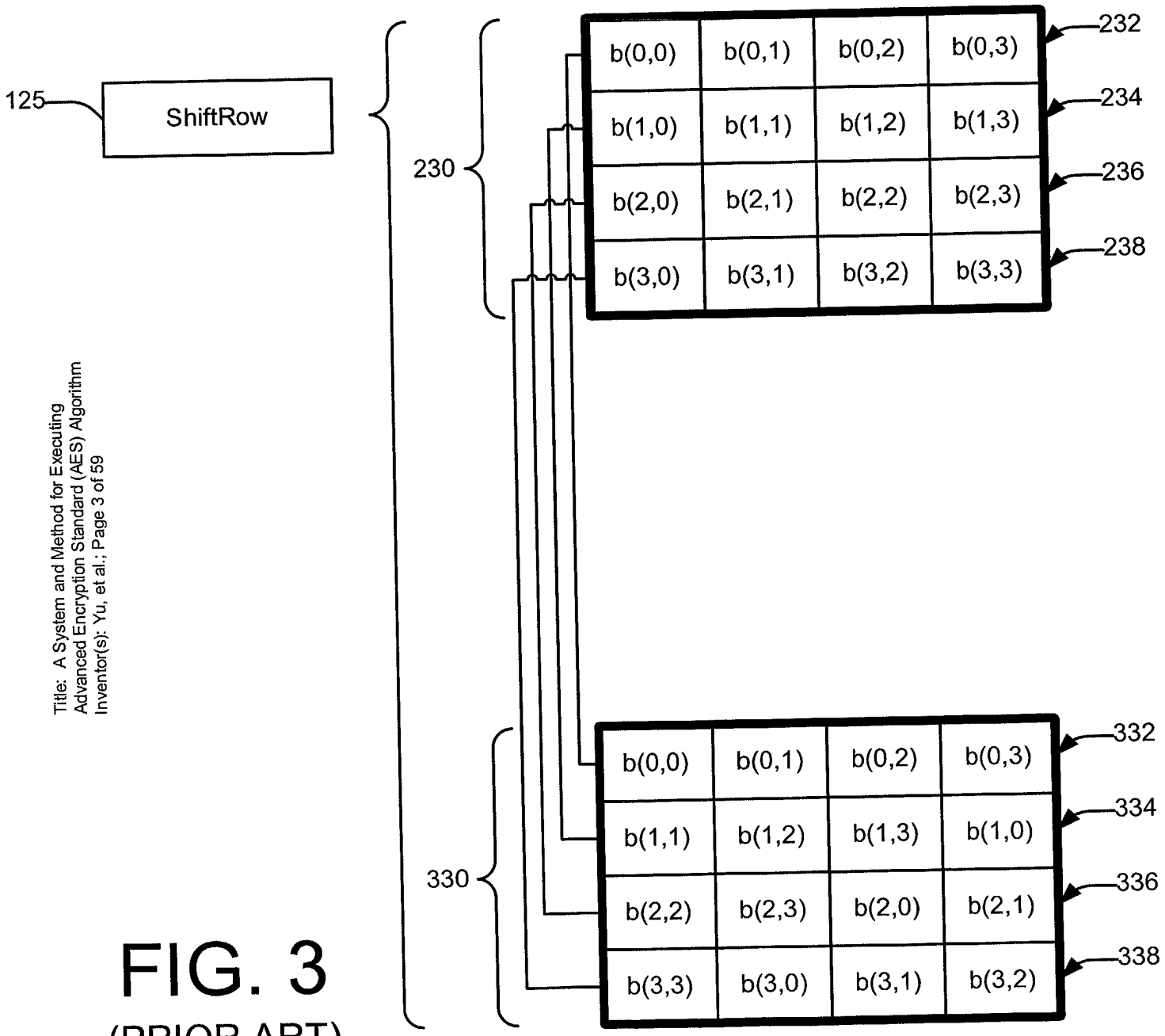


FIG. 3
(PRIOR ART)

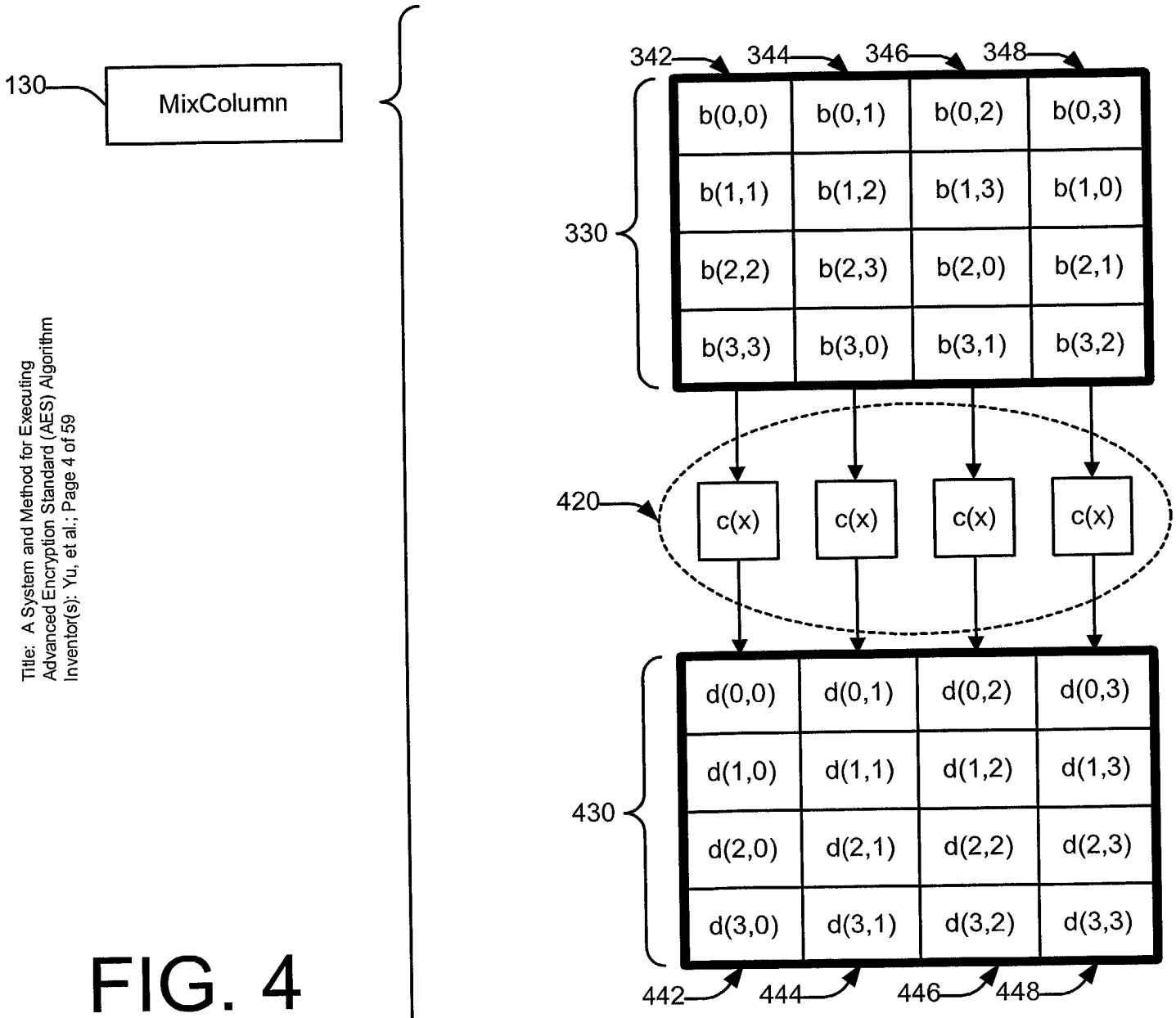


FIG. 4
(PRIOR ART)

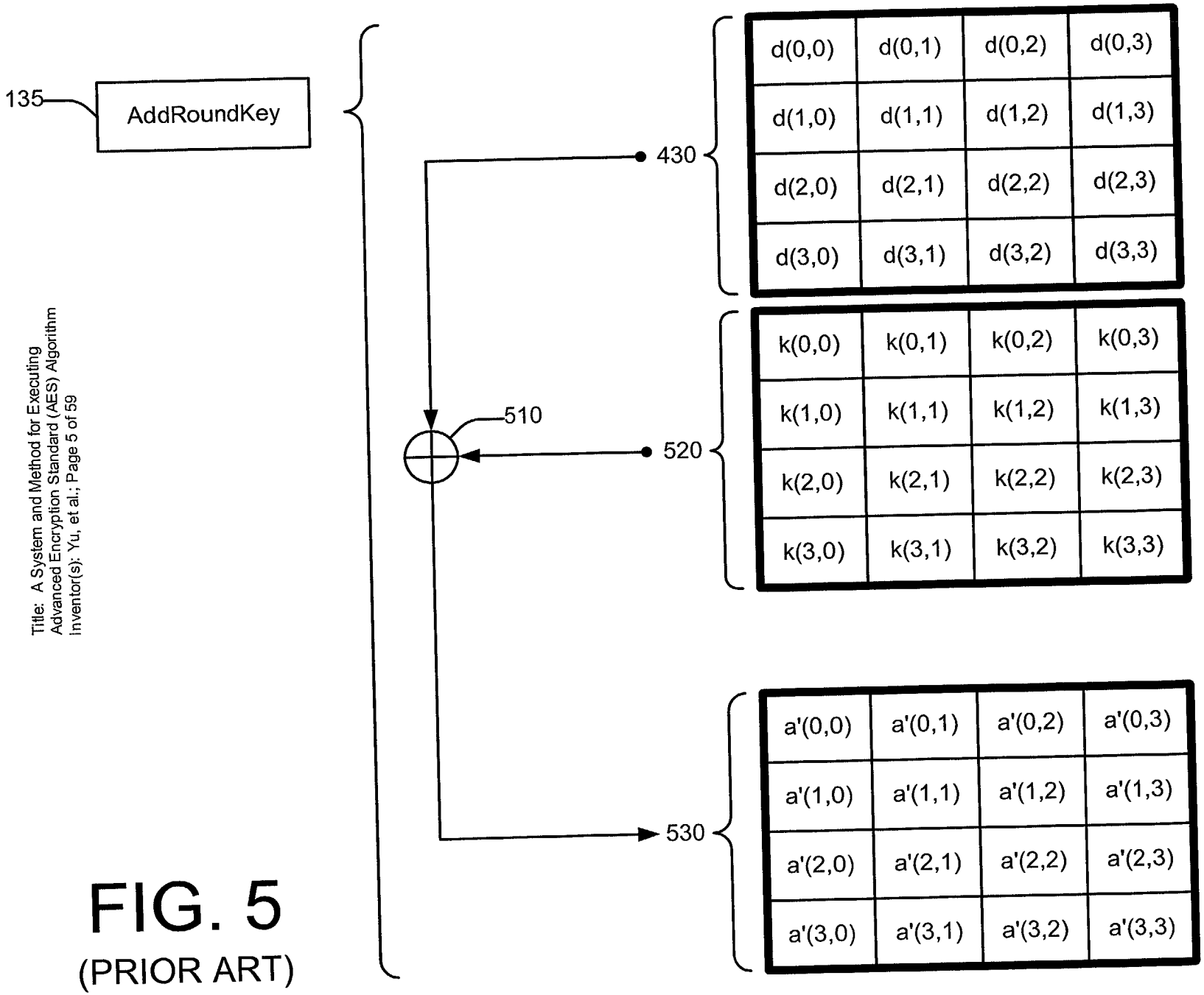


FIG. 5
(PRIOR ART)

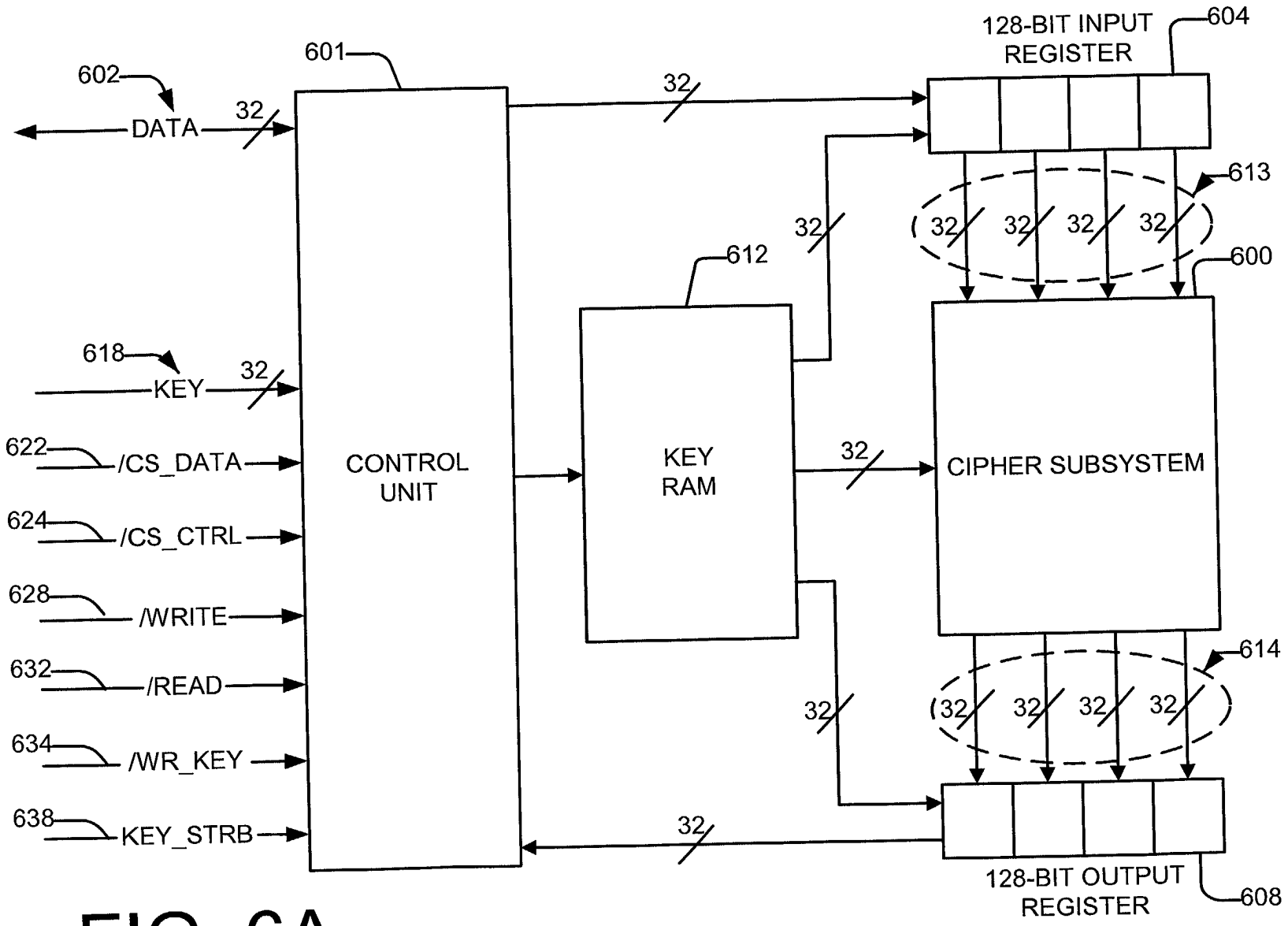


FIG. 6A
(PRIOR ART)

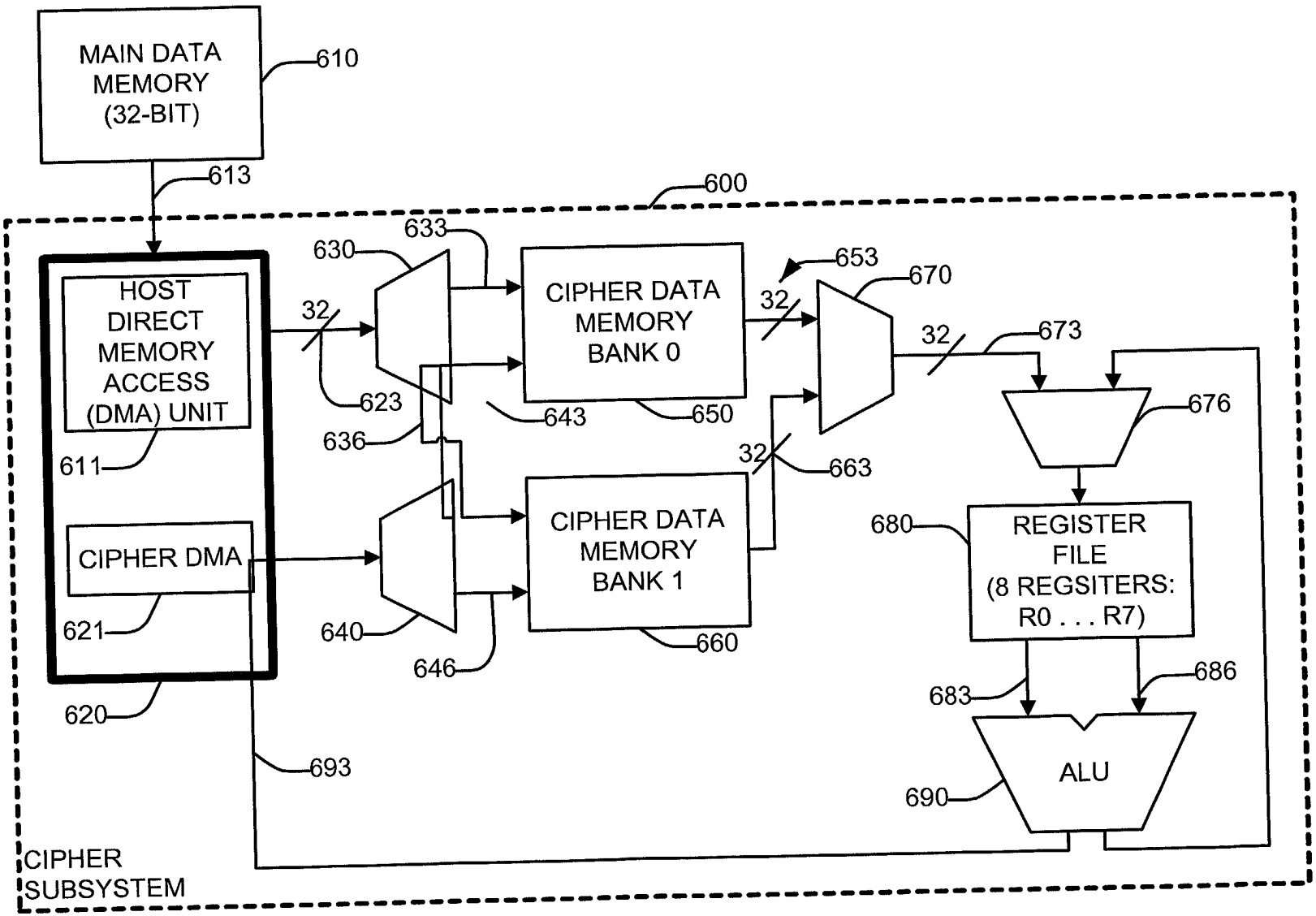


FIG. 6B
(PRIOR ART)

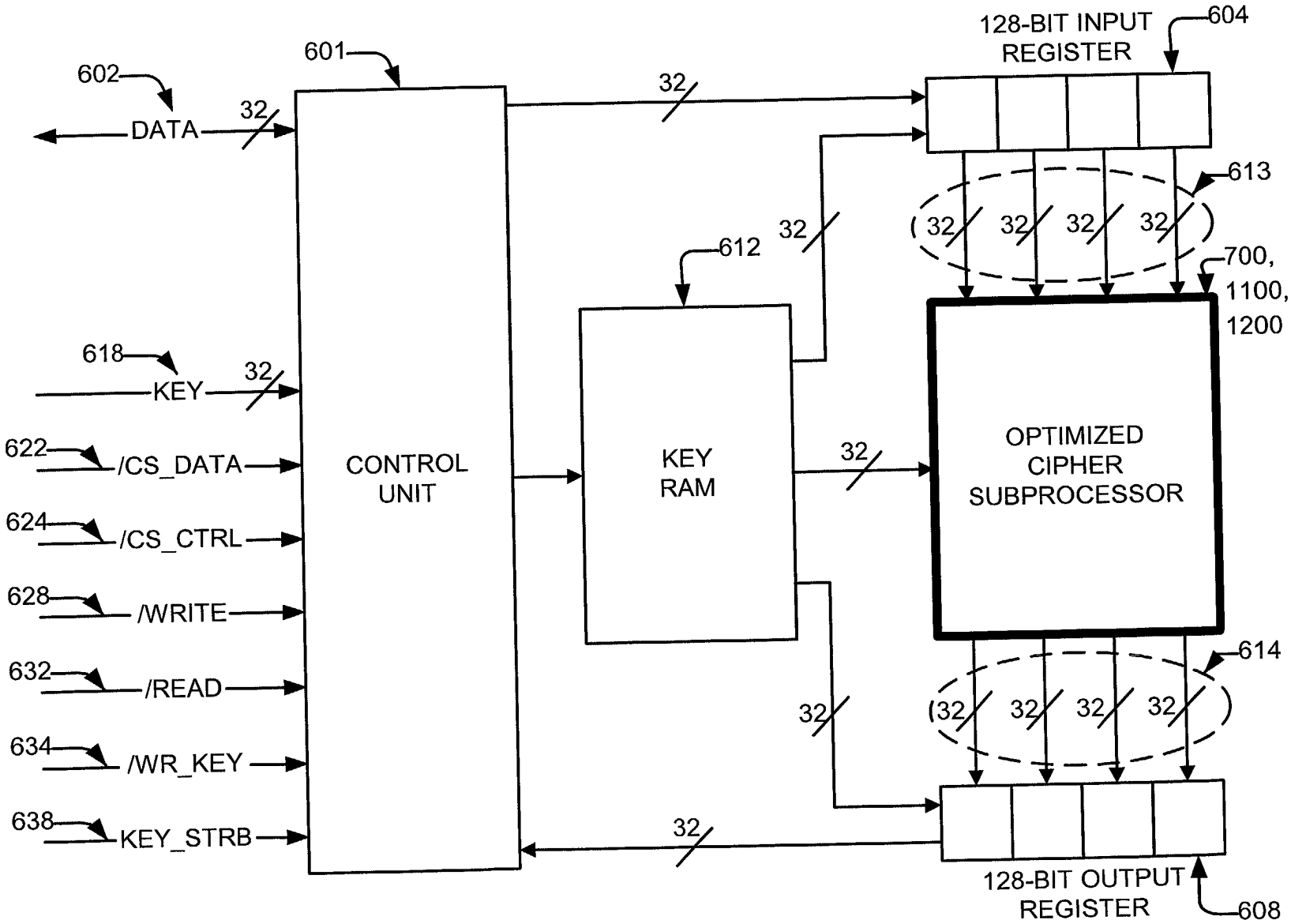

601
602
DATA
32
CONTROL UNIT
618
KEY
622
/CS_DATA
624
/CS_CTRL
628
/WRITE
632
/READ
634
/WR_KEY
638
KEY_STRB
612
KEY RAM
128-BIT INPUT REGISTER
604
613
700, 1100, 1200
OPTIMIZED CIPHER SUBPROCESSOR
614
128-BIT OUTPUT REGISTER
608

FIG. 7

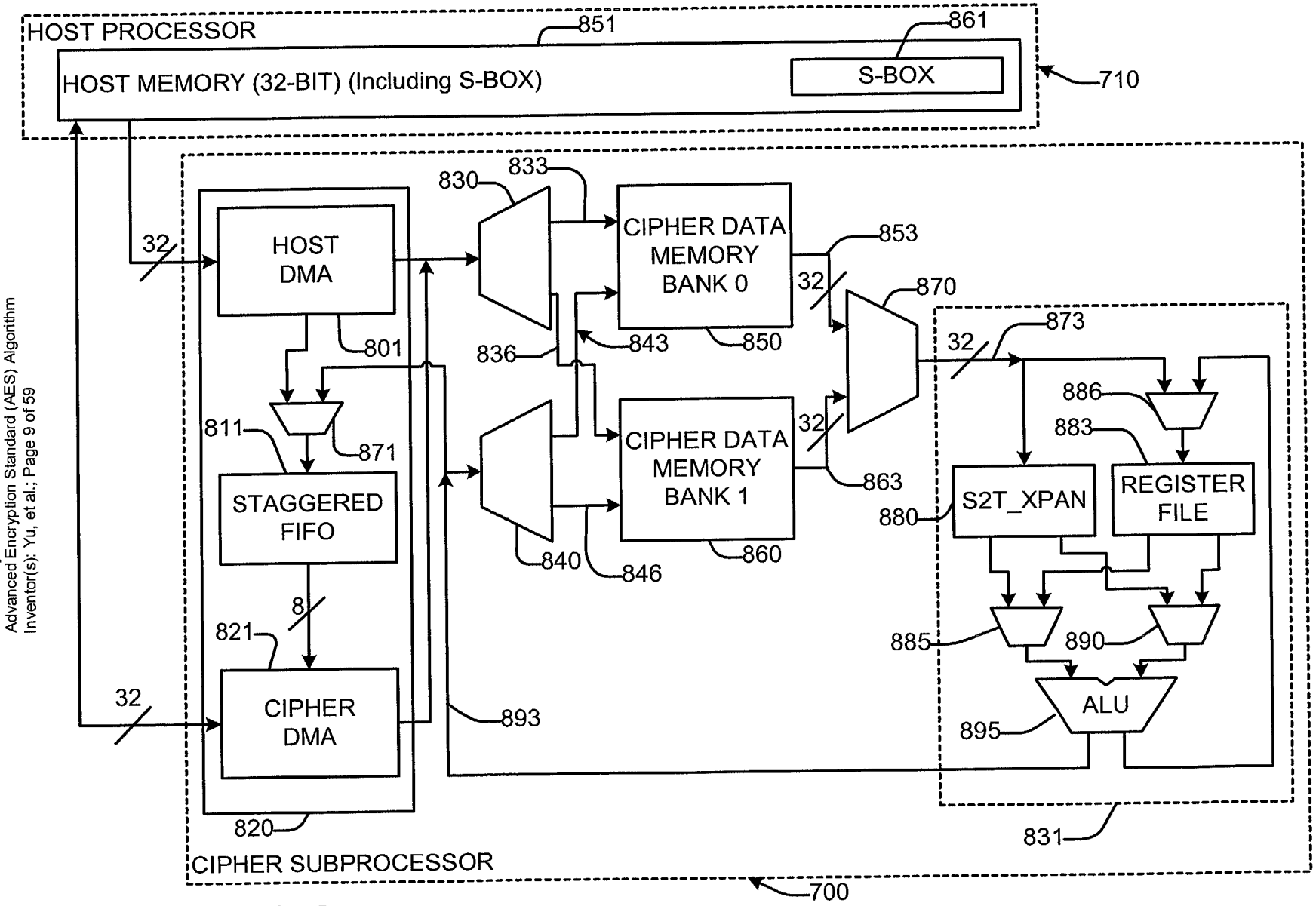

HOST PROCESSOR
851
861
HOST MEMORY (32-BIT) (Including S-BOX)
S-BOX
710
830
833
HOST DMA
32
801
CIPHER DATA MEMORY BANK 0
853
32
870
836
843
850
873
32
811
871
886
883
CIPHER DATA MEMORY BANK 1
32
863
STAGGERED FIFO
S2T_XPAN
REGISTER FILE
880
840
846
860
8
821
885
890
ALU
895
32
CIPHER DMA
893
820
831
CIPHER SUBPROCESSOR
700

FIG. 8A

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 10 of 59

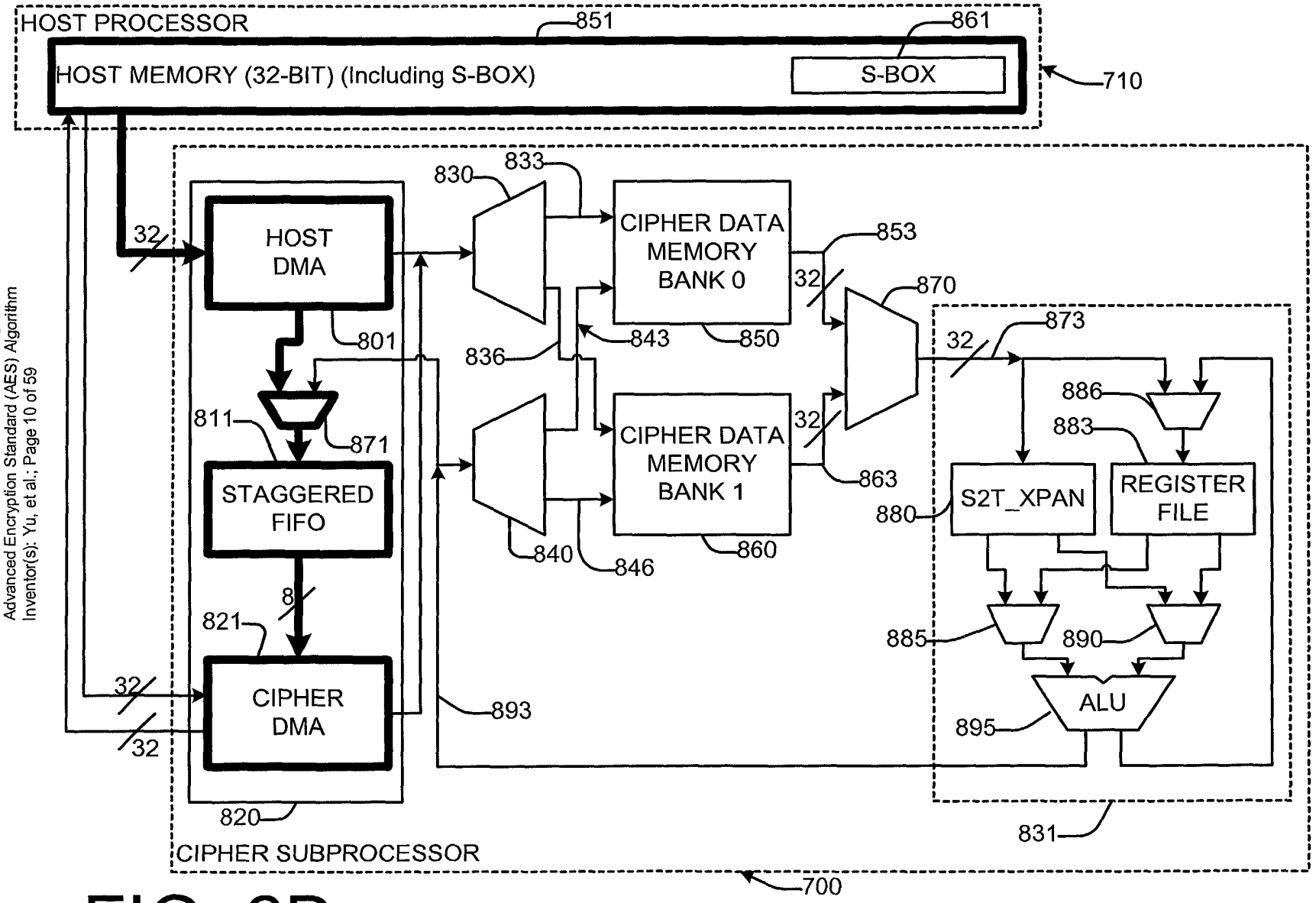


FIG. 8B

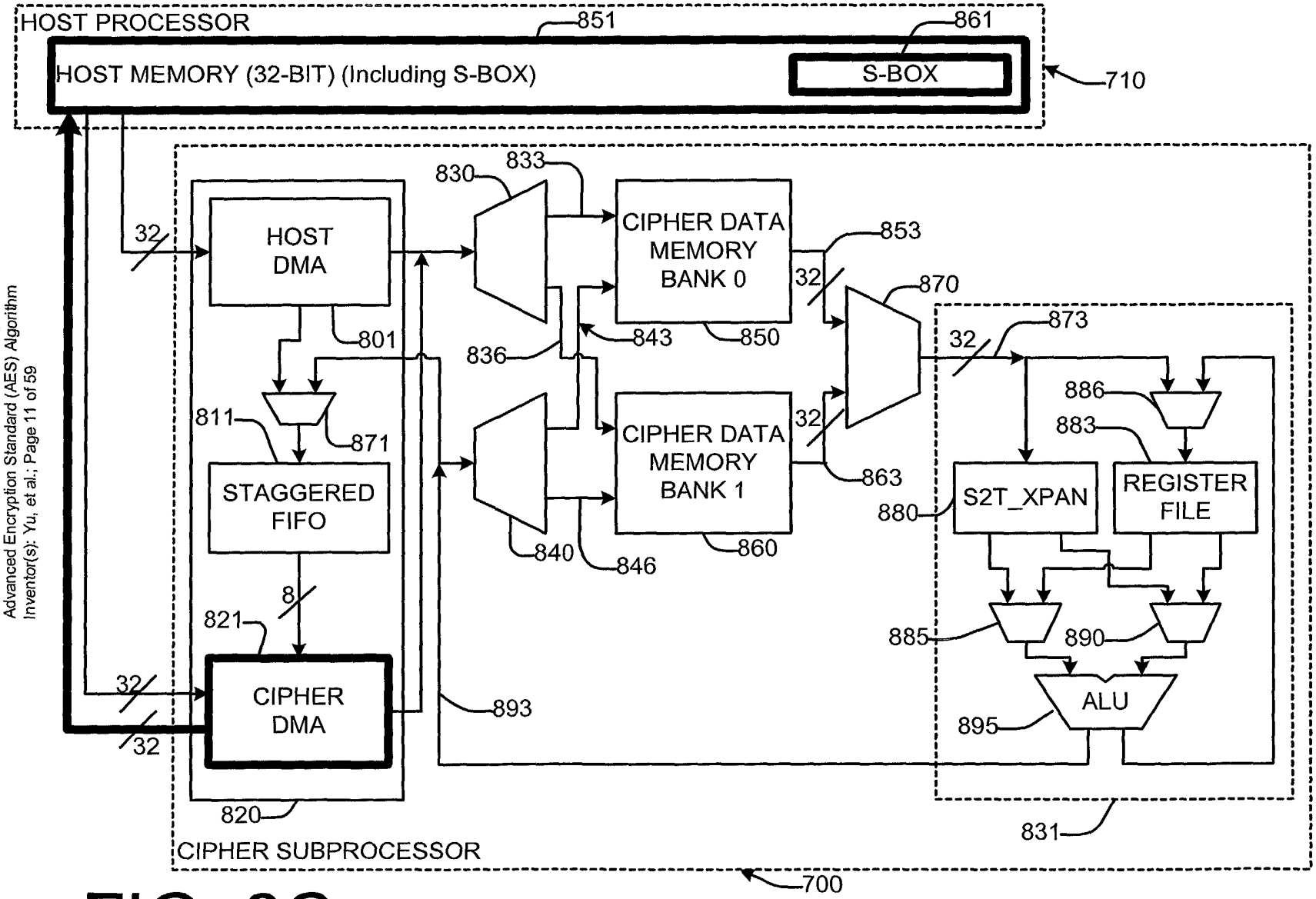

HOST PROCESSOR
851
861
HOST MEMORY (32-BIT) (Including S-BOX)
S-BOX
710
830
833
HOST DMA
32
801
CIPHER DATA MEMORY BANK 0
853
32
870
836
843
850
873
32
811
871
886
883
CIPHER DATA MEMORY BANK 1
32
863
STAGGERED FIFO
880
S2T_XPAN
REGISTER FILE
840
846
860
8
821
885
890
32
CIPHER DMA
893
ALU
895
32
820
831
CIPHER SUBPROCESSOR
700

FIG. 8C

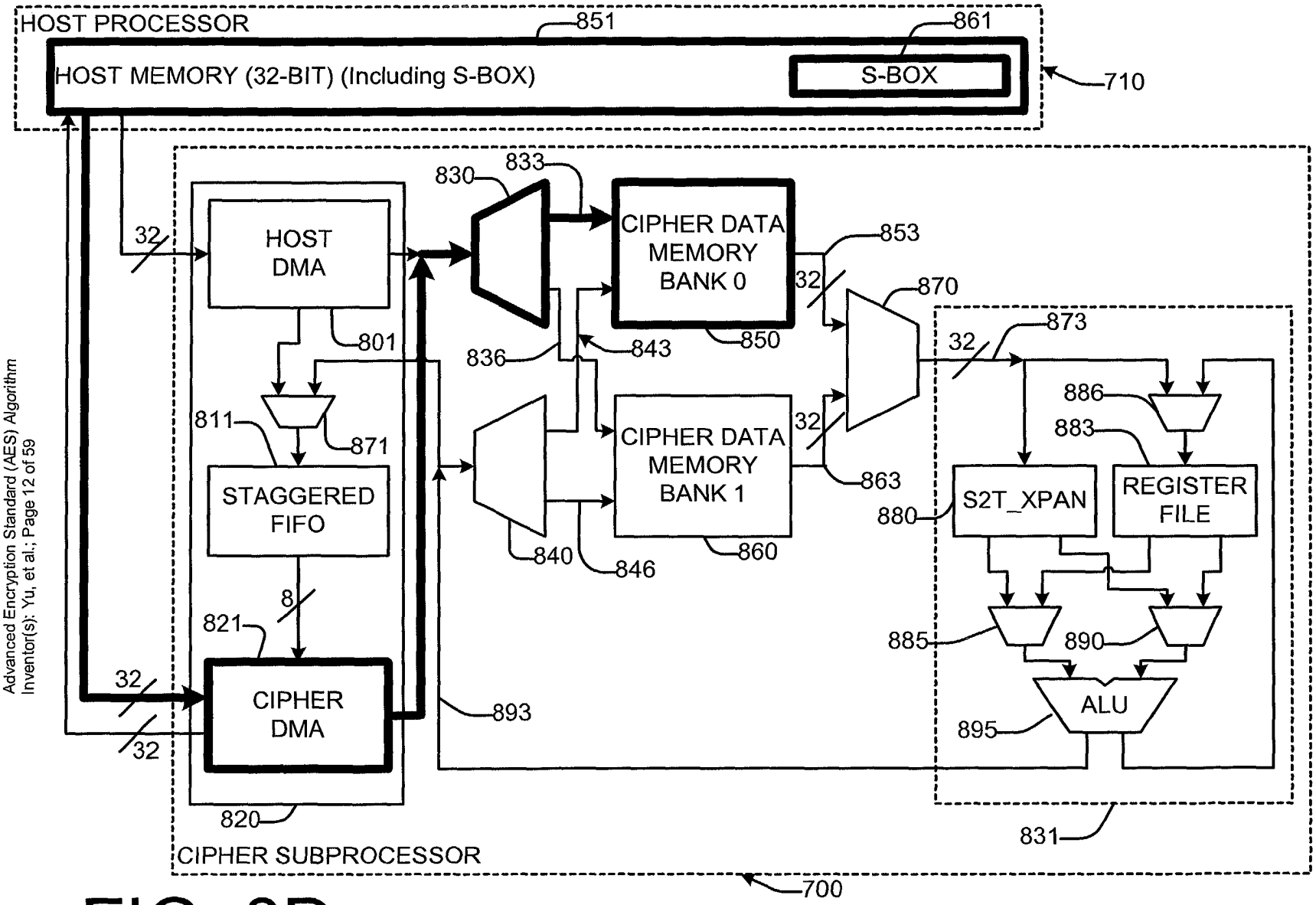


FIG. 8D

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 12 of 59

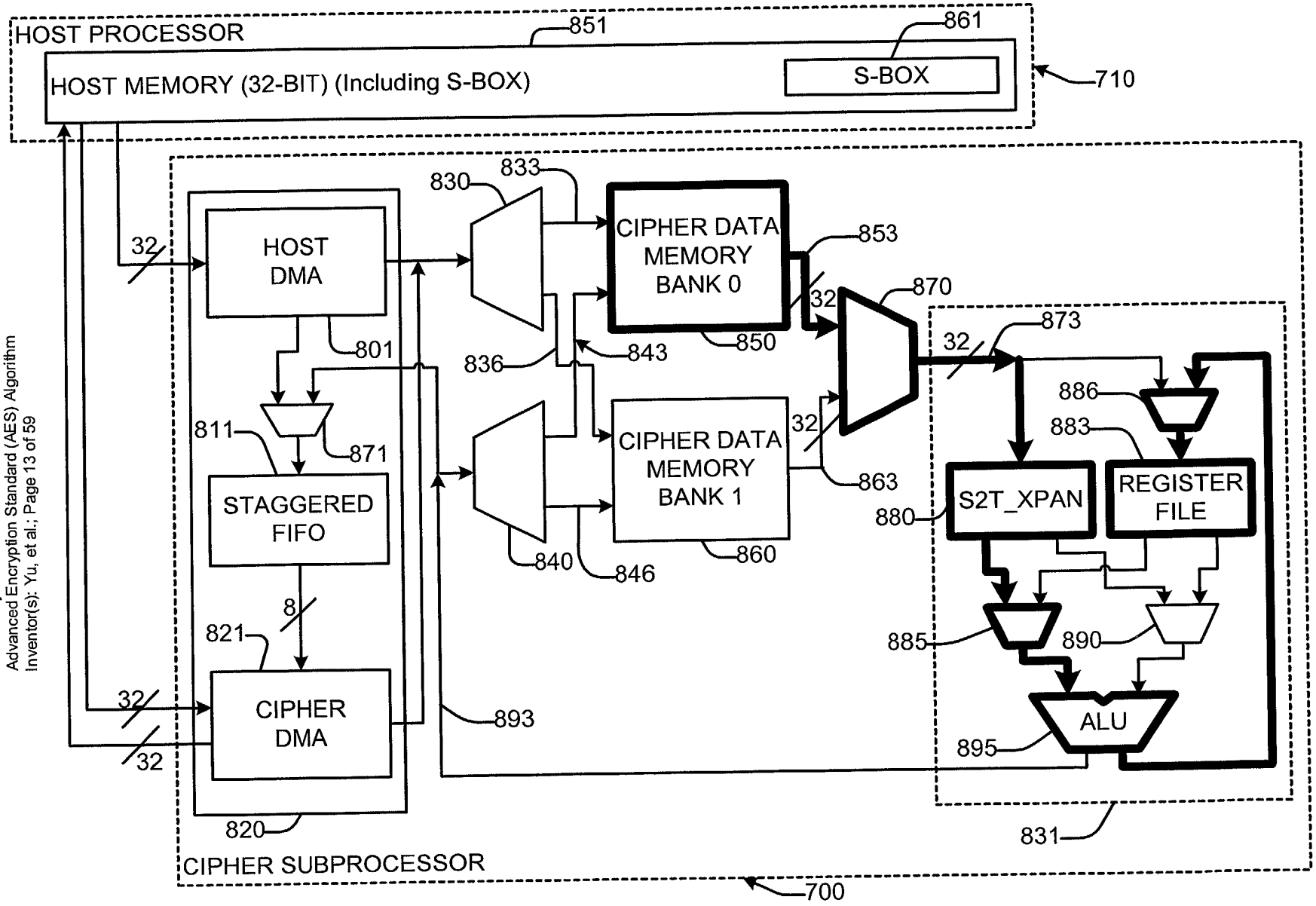


FIG. 8E

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 13 of 59

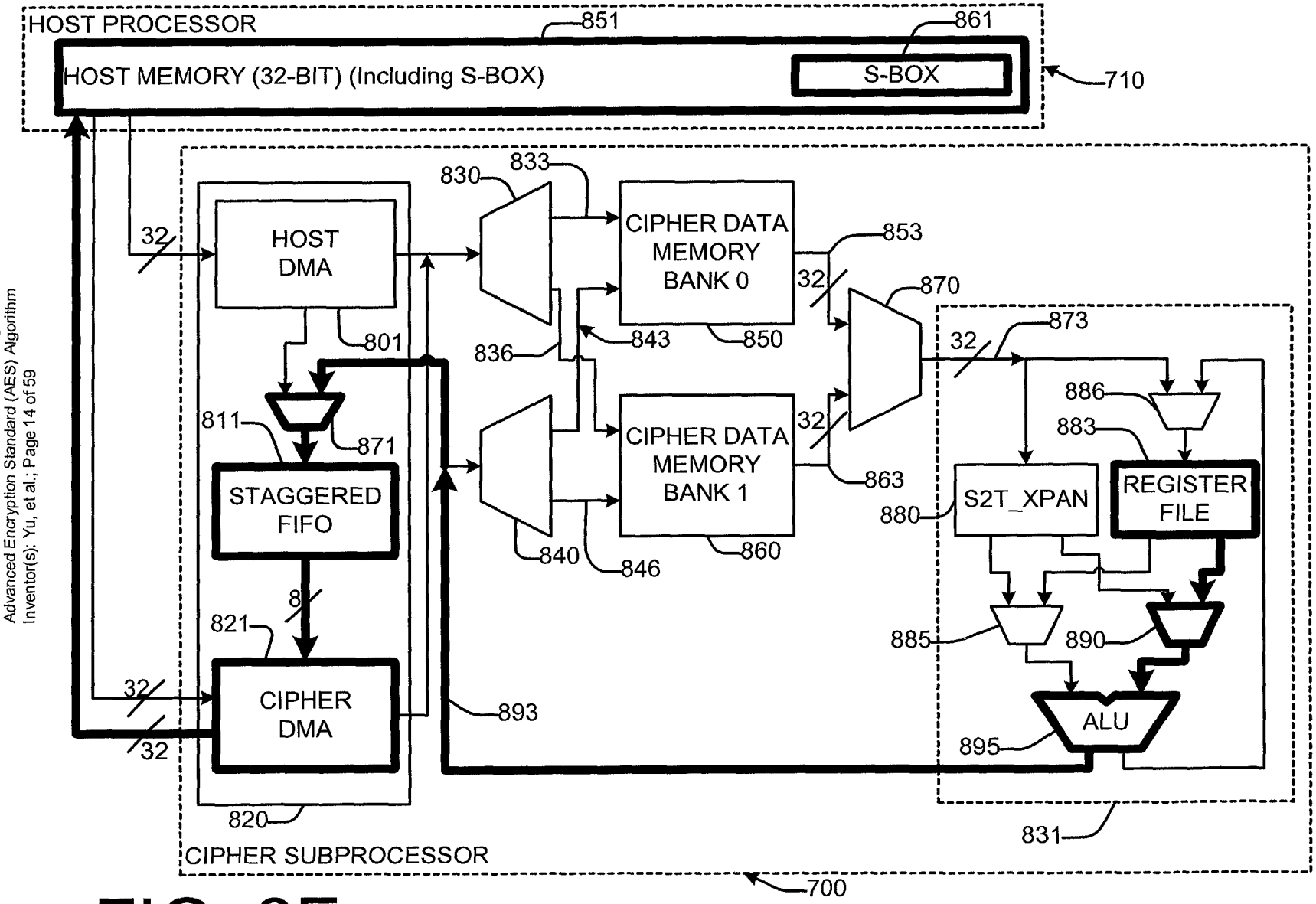


FIG. 8F

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 14 of 59

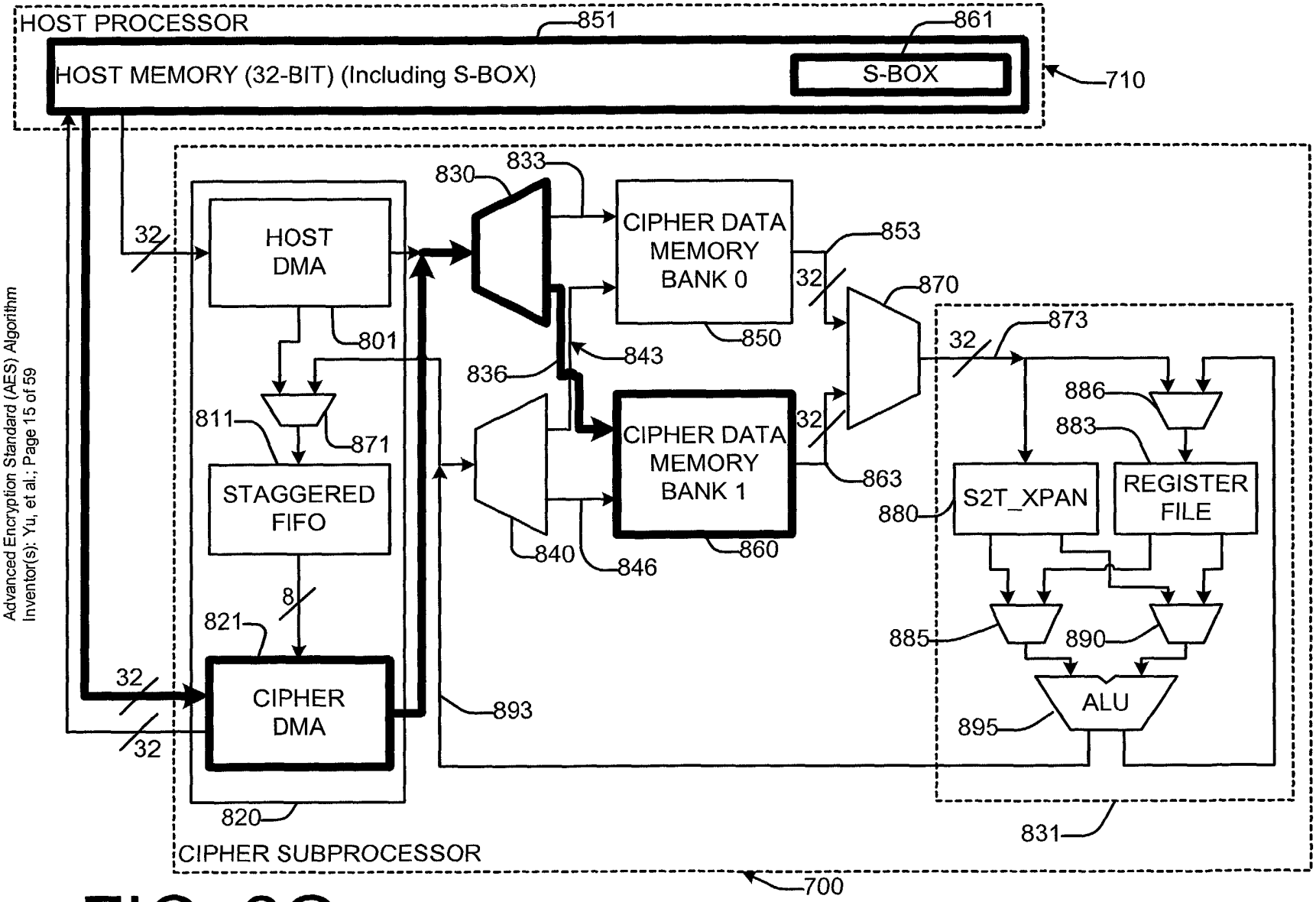

HOST PROCESSOR
851
861
HOST MEMORY (32-BIT) (Including S-BOX)
S-BOX
710
830
833
HOST DMA
32
801
CIPHER DATA MEMORY BANK 0
853
850
843
836
811
871
STAGGERED FIFO
CIPHER DATA MEMORY BANK 1
863
860
840
846
8
821
32
CIPHER DMA
32
893
820
870
873
886
883
S2T_XPAN
REGISTER FILE
880
885
890
ALU
895
831
CIPHER SUBPROCESSOR
700

FIG. 8G

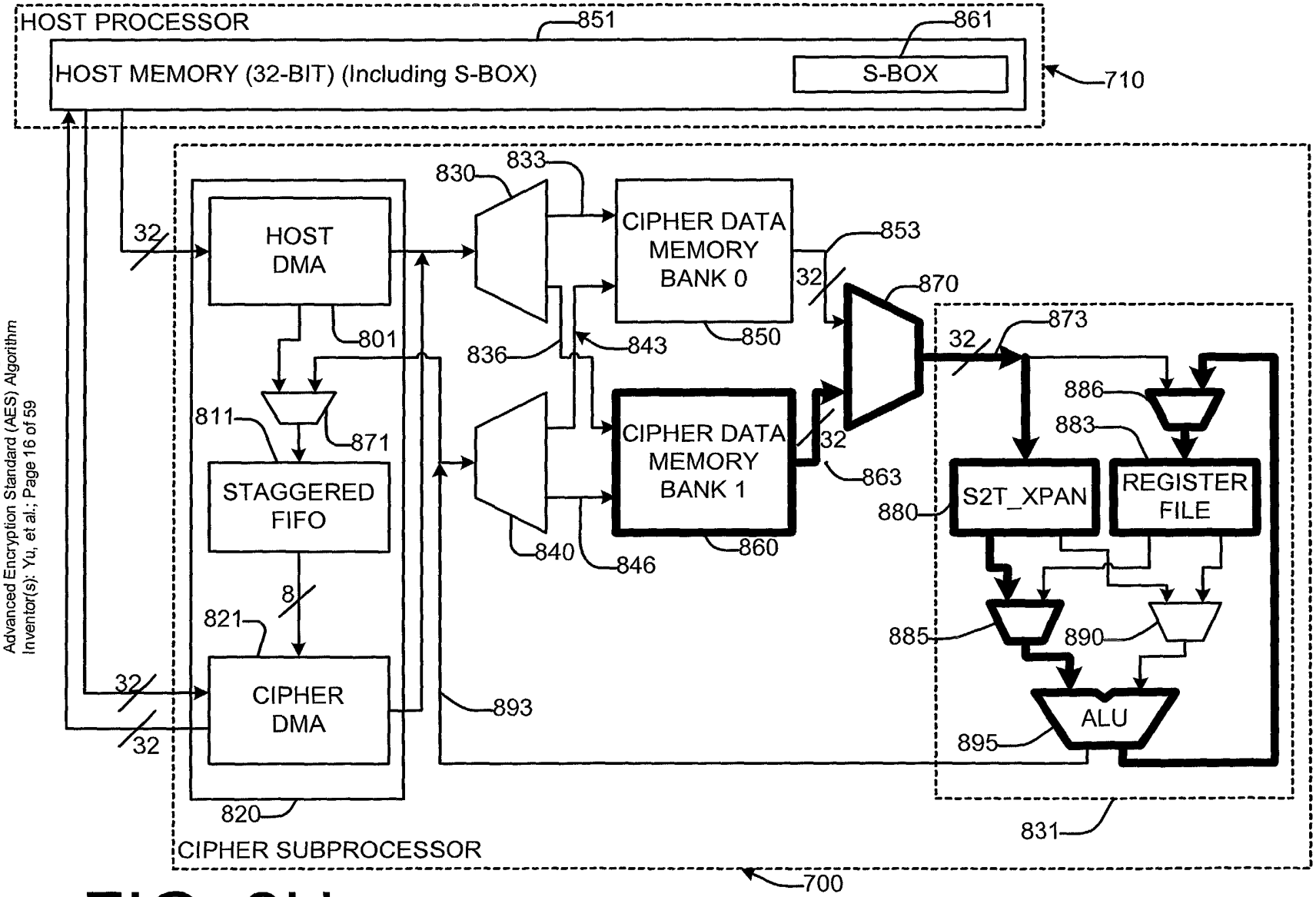


FIG. 8H

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 16 of 59

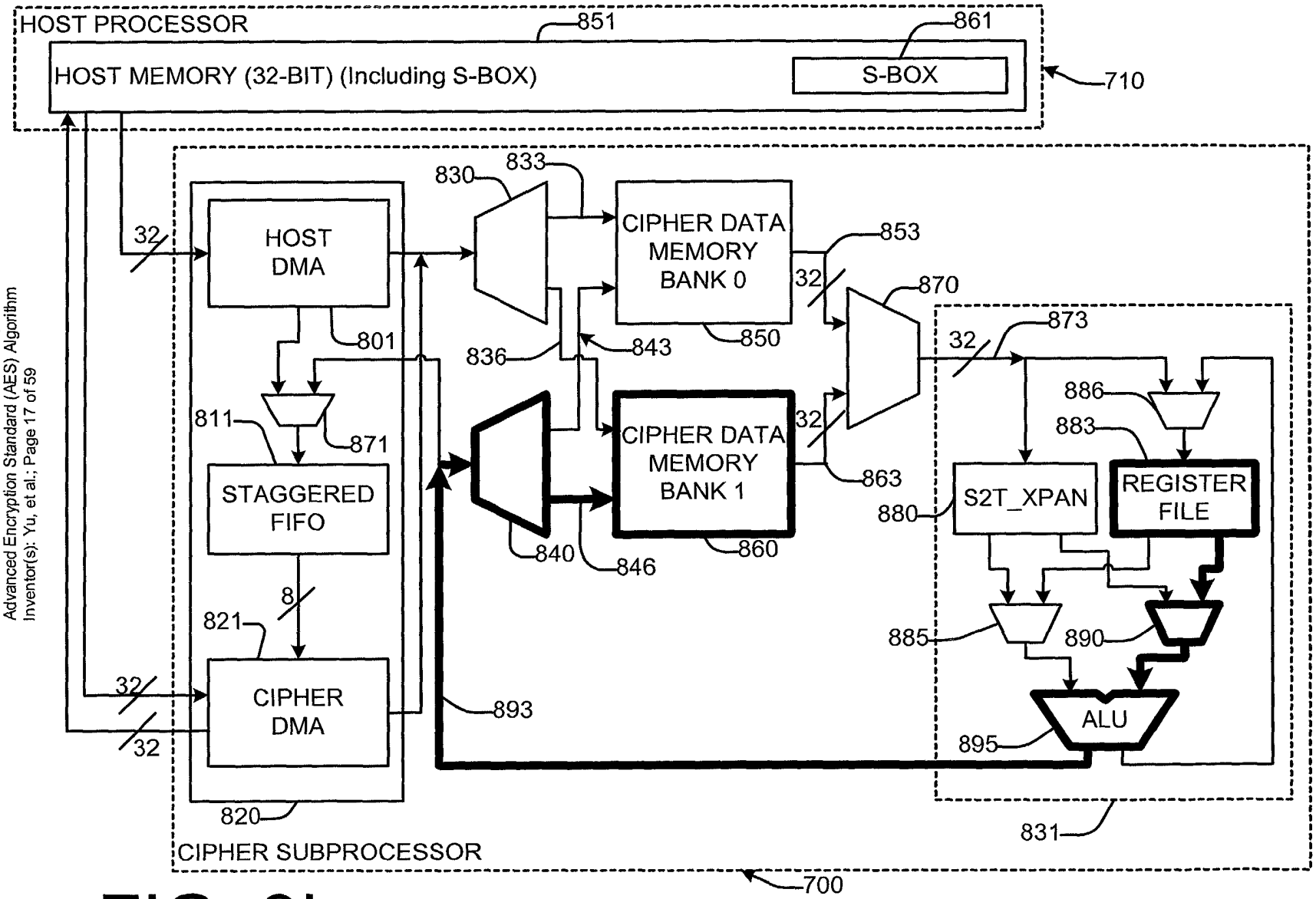

HOST PROCESSOR
851
861
HOST MEMORY (32-BIT) (Including S-BOX)
S-BOX
710
830
833
HOST DMA
32
801
CIPHER DATA MEMORY BANK 0
853
32
870
836
843
850
811
871
CIPHER DATA MEMORY BANK 1
32
863
STAGGERED FIFO
840
846
860
8
821
CIPHER DMA
32
32
893
820
CIPHER SUBPROCESSOR
700
32
873
886
883
S2T_XPAN
REGISTER FILE
880
885
890
ALU
895
831

FIG. 8I

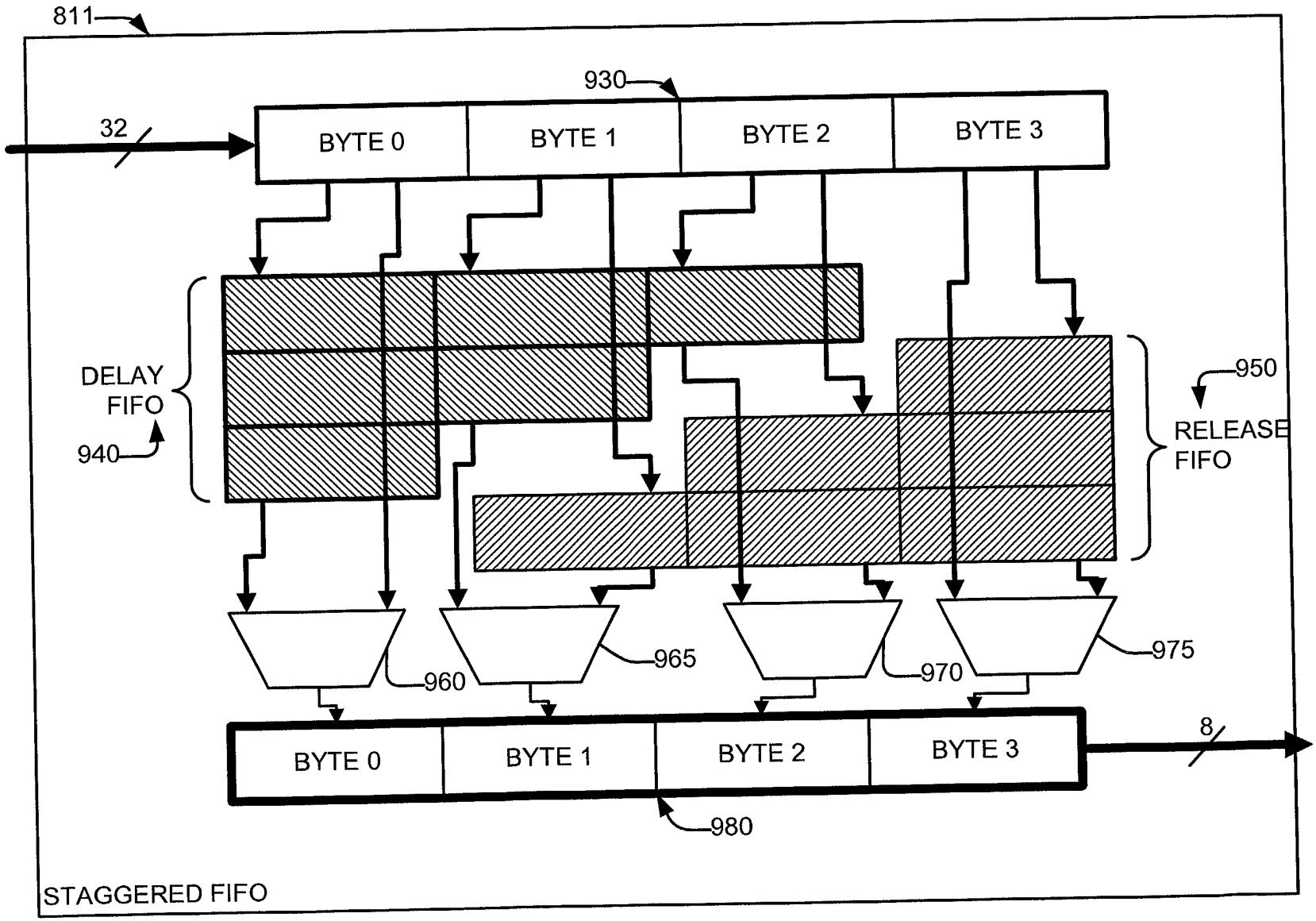

811
930
32
BYTE 0
BYTE 1
BYTE 2
BYTE 3
DELAY FIFO
940
950
RELEASE FIFO
960
965
970
975
8
BYTE 0
BYTE 1
BYTE 2
BYTE 3
980
STAGGERED FIFO

FIG. 9A

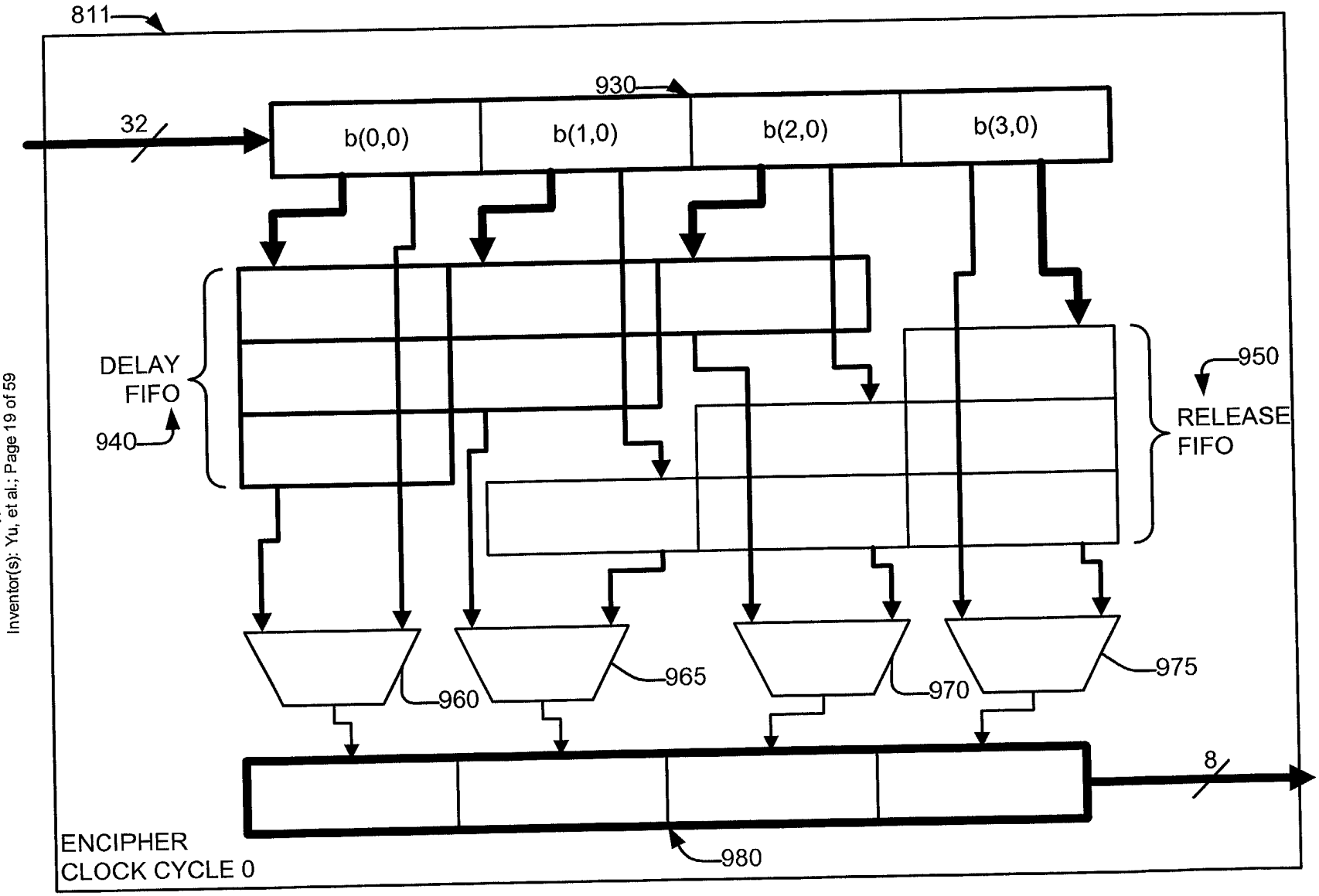

811
930
32
b(0,0)
b(1,0)
b(2,0)
b(3,0)
DELAY
FIFO
940
950
RELEASE
FIFO
960
965
970
975
8
980
ENCIPHER
CLOCK CYCLE 0

FIG. 9B

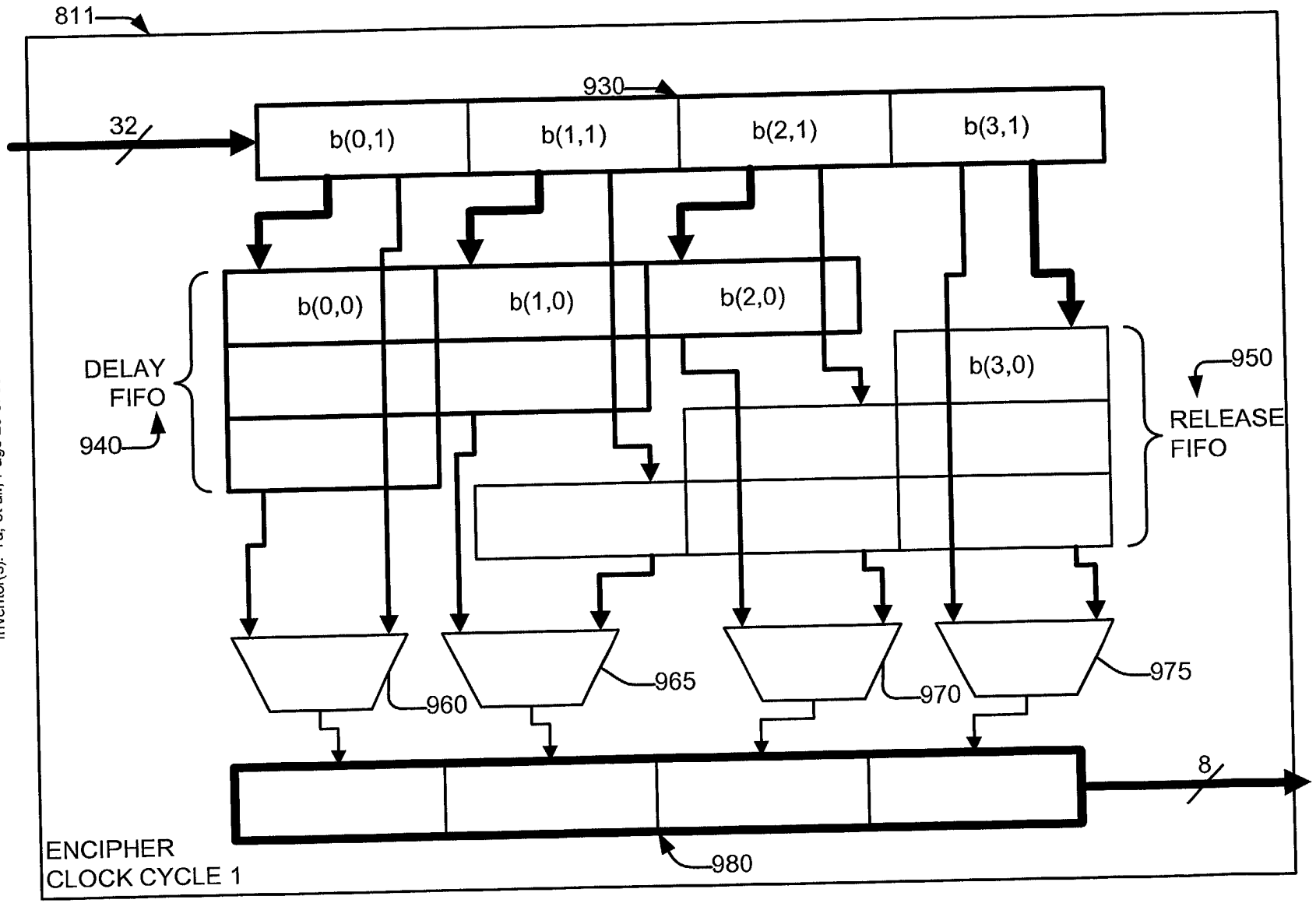

811
930
32
b(0,1)
b(1,1)
b(2,1)
b(3,1)
b(0,0)
b(1,0)
b(2,0)
b(3,0)
DELAY
FIFO
940
950
RELEASE
FIFO
960
965
970
975
8
980
ENCIPHER
CLOCK CYCLE 1

FIG. 9C

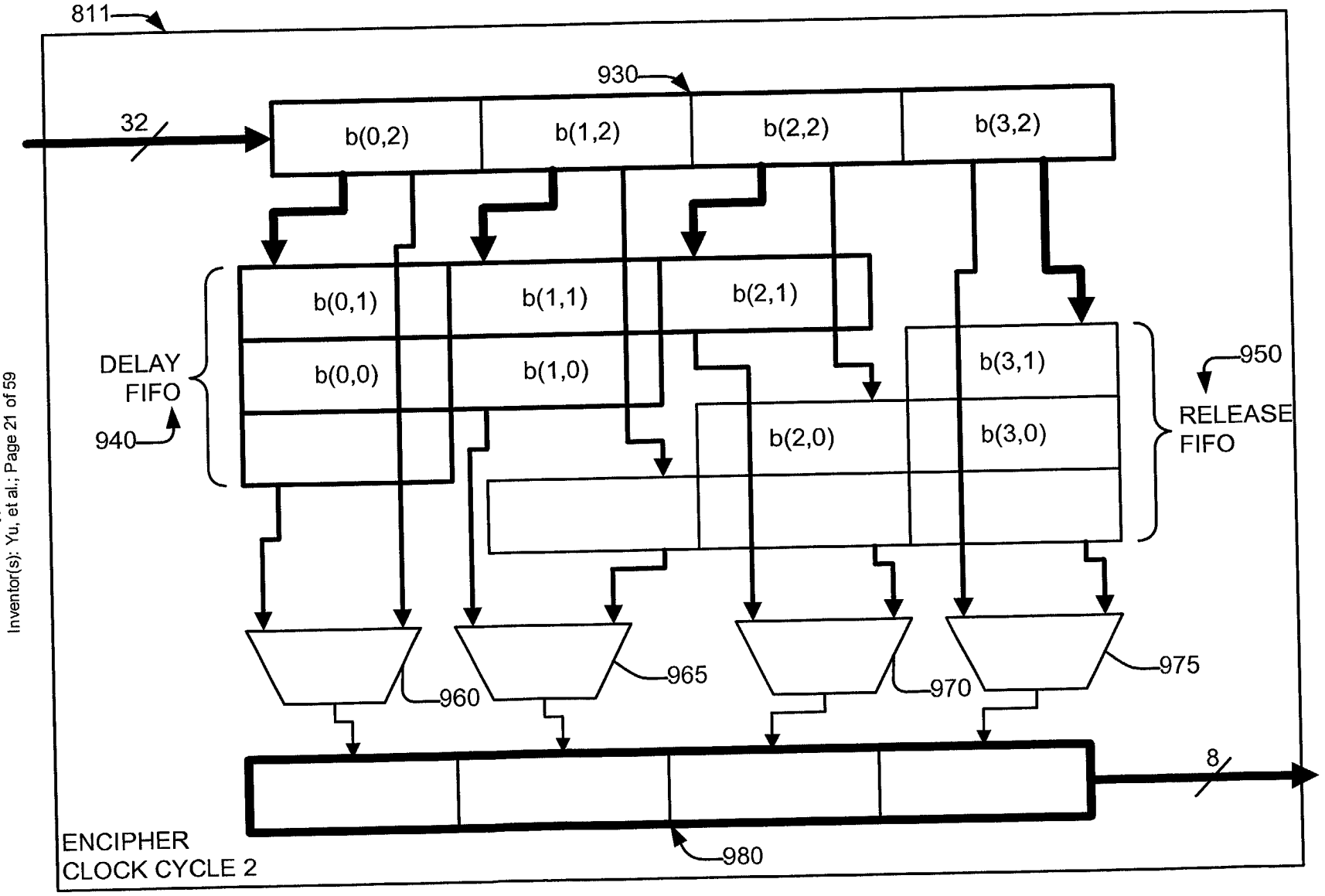

811
930
32
b(0,2)
b(1,2)
b(2,2)
b(3,2)
b(0,1)
b(1,1)
b(2,1)
b(3,1)
DELAY
FIFO
940
b(0,0)
b(1,0)
b(2,0)
b(3,0)
950
RELEASE
FIFO
960
965
970
975
8
980
ENCIPHER
CLOCK CYCLE 2

FIG. 9D

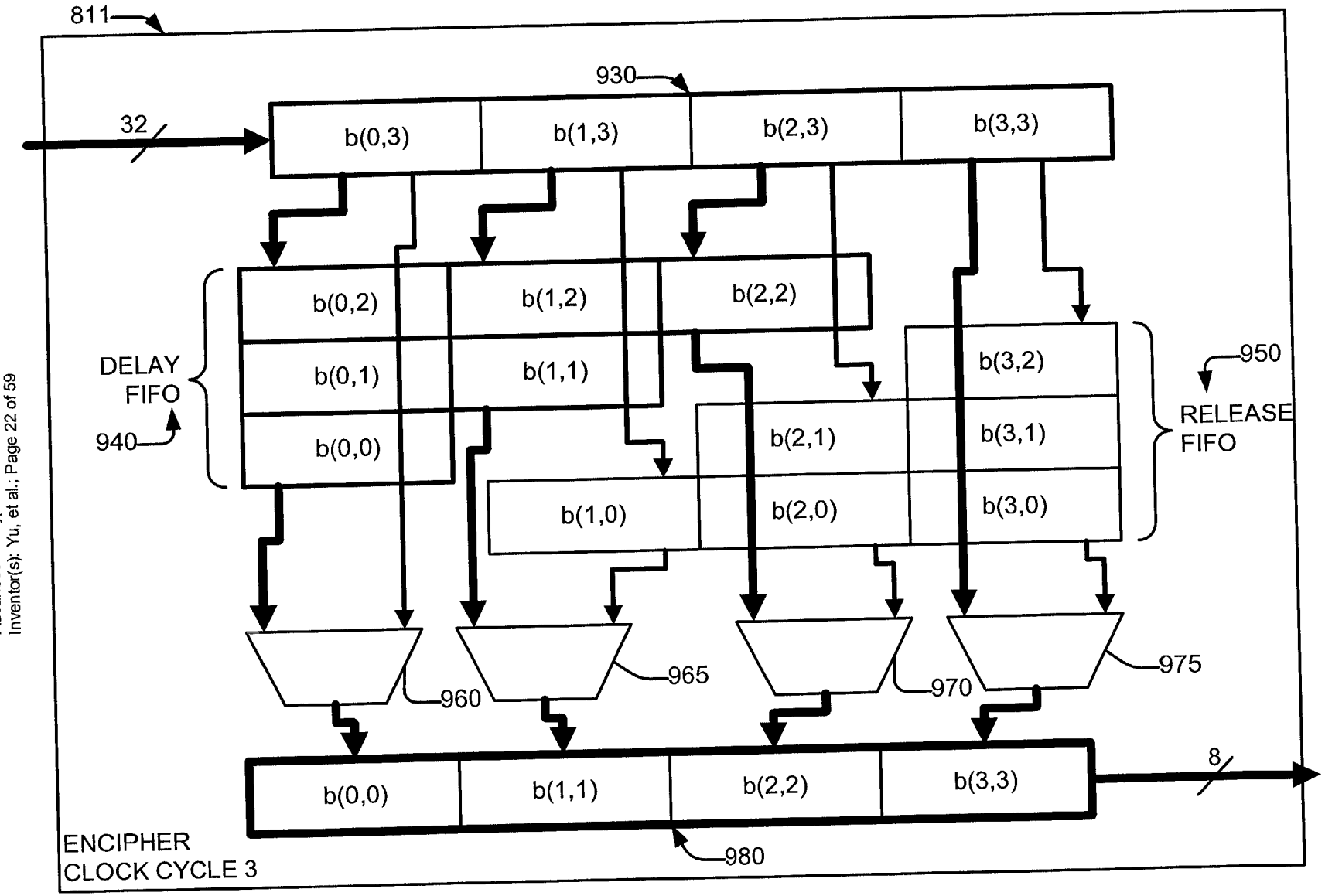

811
930
32
b(0,3)
b(1,3)
b(2,3)
b(3,3)
b(0,2)
b(1,2)
b(2,2)
b(3,2)
DELAY
FIFO
940
b(0,1)
b(1,1)
b(2,1)
b(3,1)
950
RELEASE
FIFO
b(0,0)
b(1,0)
b(2,0)
b(3,0)
960
965
970
975
8
b(0,0)
b(1,1)
b(2,2)
b(3,3)
980
ENCIPHER
CLOCK CYCLE 3

FIG. 9E

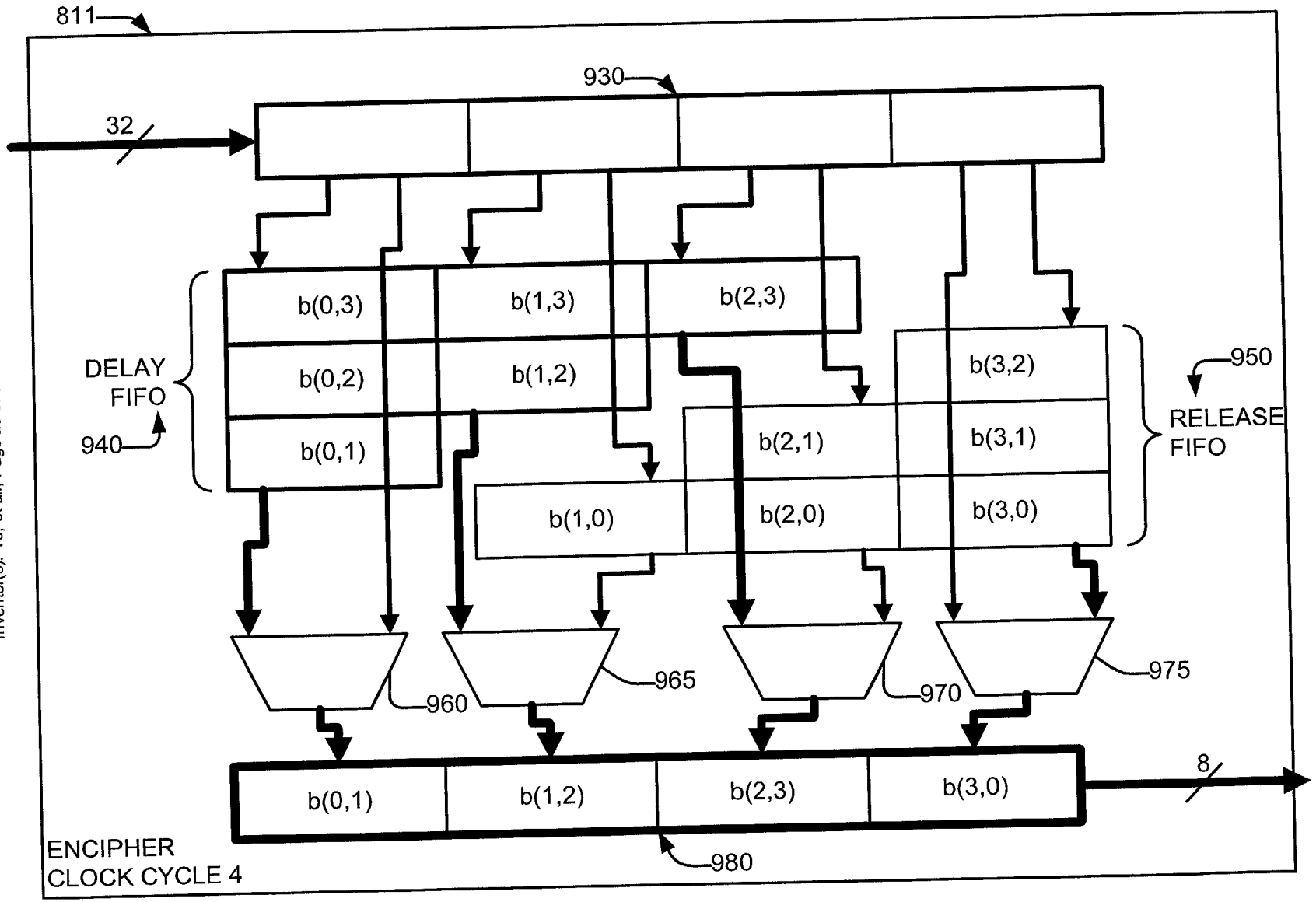

811
930
32
b(0,3)
b(1,3)
b(2,3)
b(3,2)
DELAY
FIFO
940
b(0,2)
b(1,2)
b(0,1)
b(2,1)
b(3,1)
950
RELEASE
FIFO
b(1,0)
b(2,0)
b(3,0)
960
965
970
975
8
b(0,1)
b(1,2)
b(2,3)
b(3,0)
980
ENCIPHER
CLOCK CYCLE 4

FIG. 9F

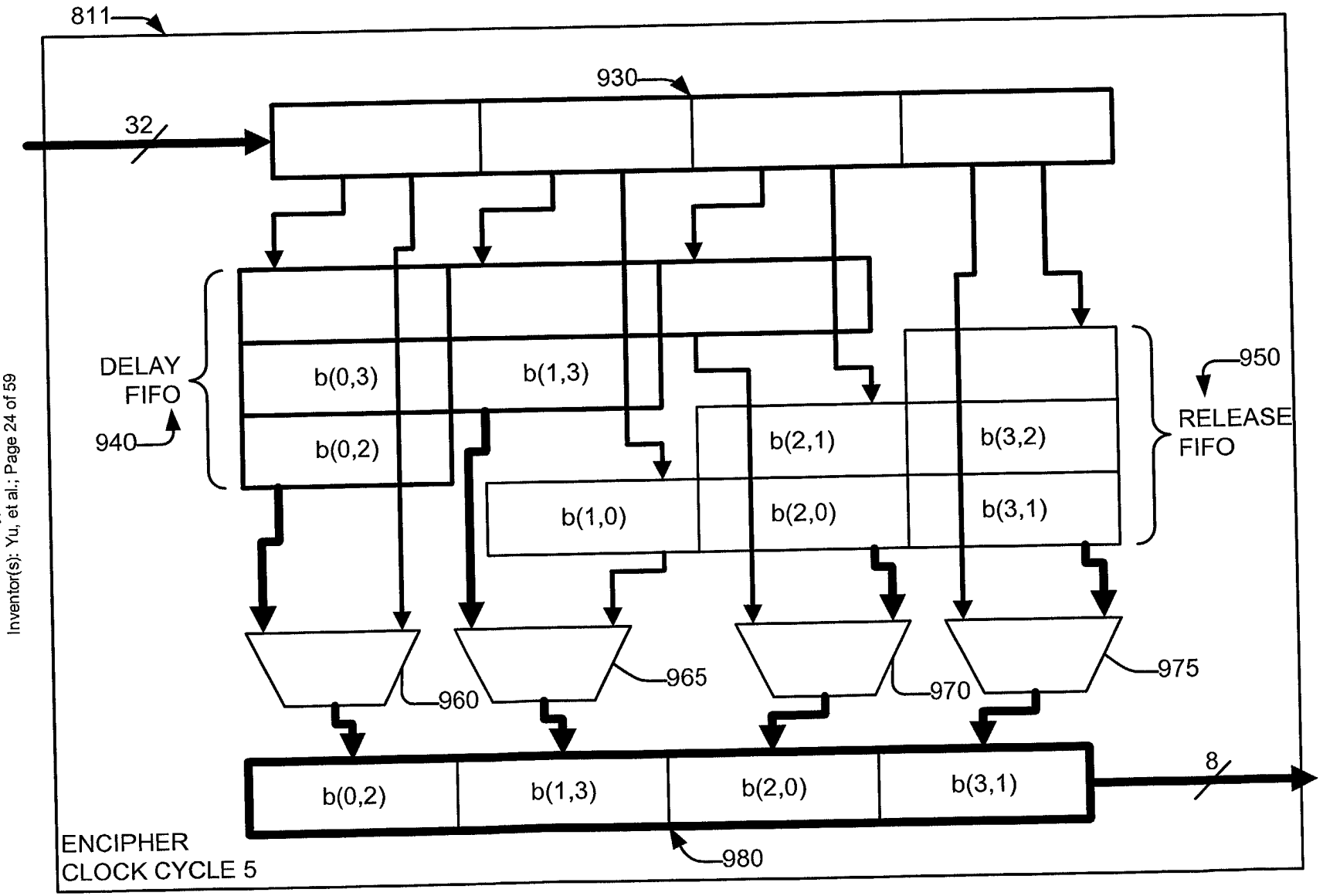

811
930
32
DELAY
FIFO
940
b(0,3)
b(1,3)
b(0,2)
b(2,1)
b(3,2)
b(1,0)
b(2,0)
b(3,1)
950
RELEASE
FIFO
960
965
970
975
8
b(0,2)
b(1,3)
b(2,0)
b(3,1)
980
ENCIPHER
CLOCK CYCLE 5

FIG. 9G

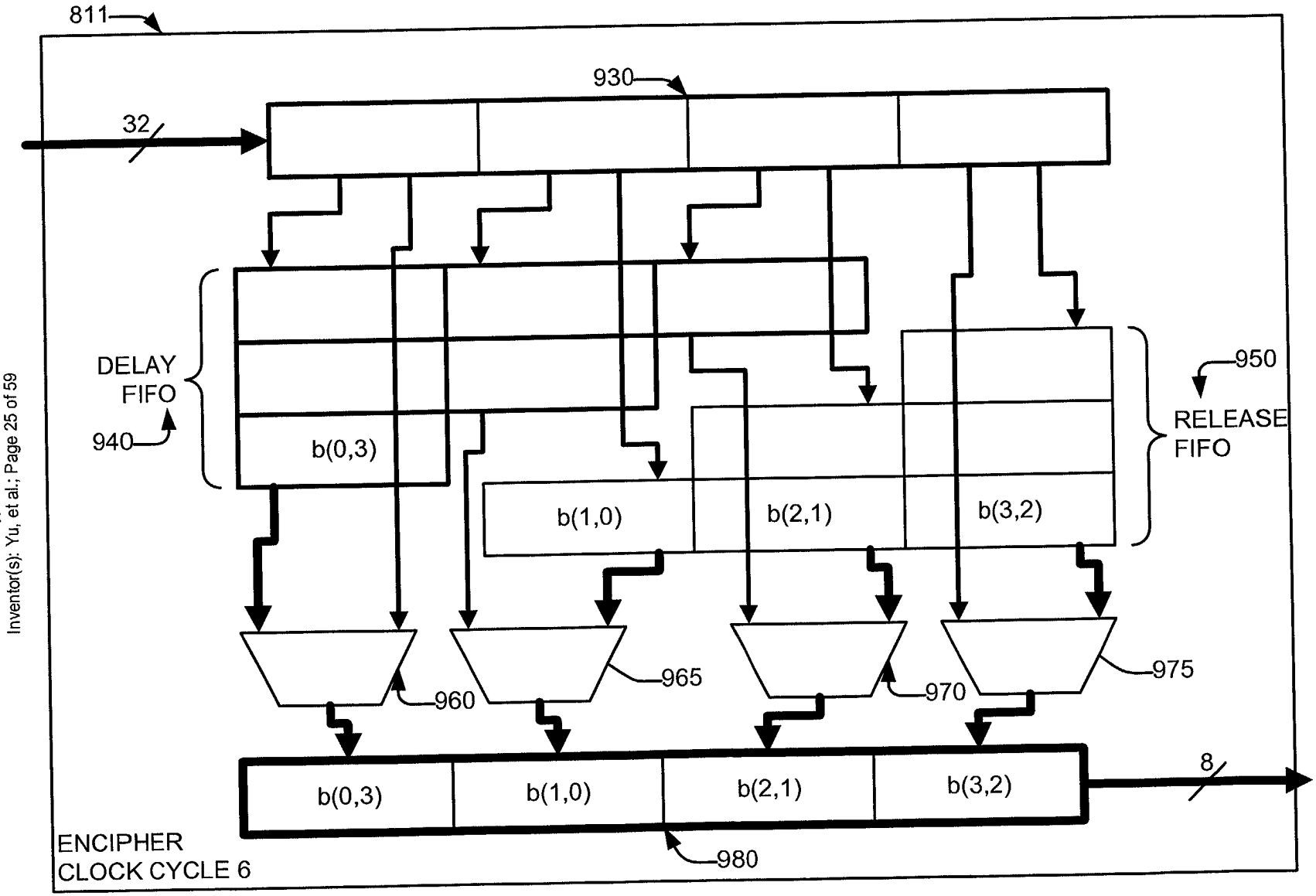

811
930
32
DELAY
FIFO
940
b(0,3)
950
RELEASE
FIFO
b(1,0)
b(2,1)
b(3,2)
960
965
970
975
8
b(0,3)
b(1,0)
b(2,1)
b(3,2)
980
ENCIPHER
CLOCK CYCLE 6

FIG. 9H

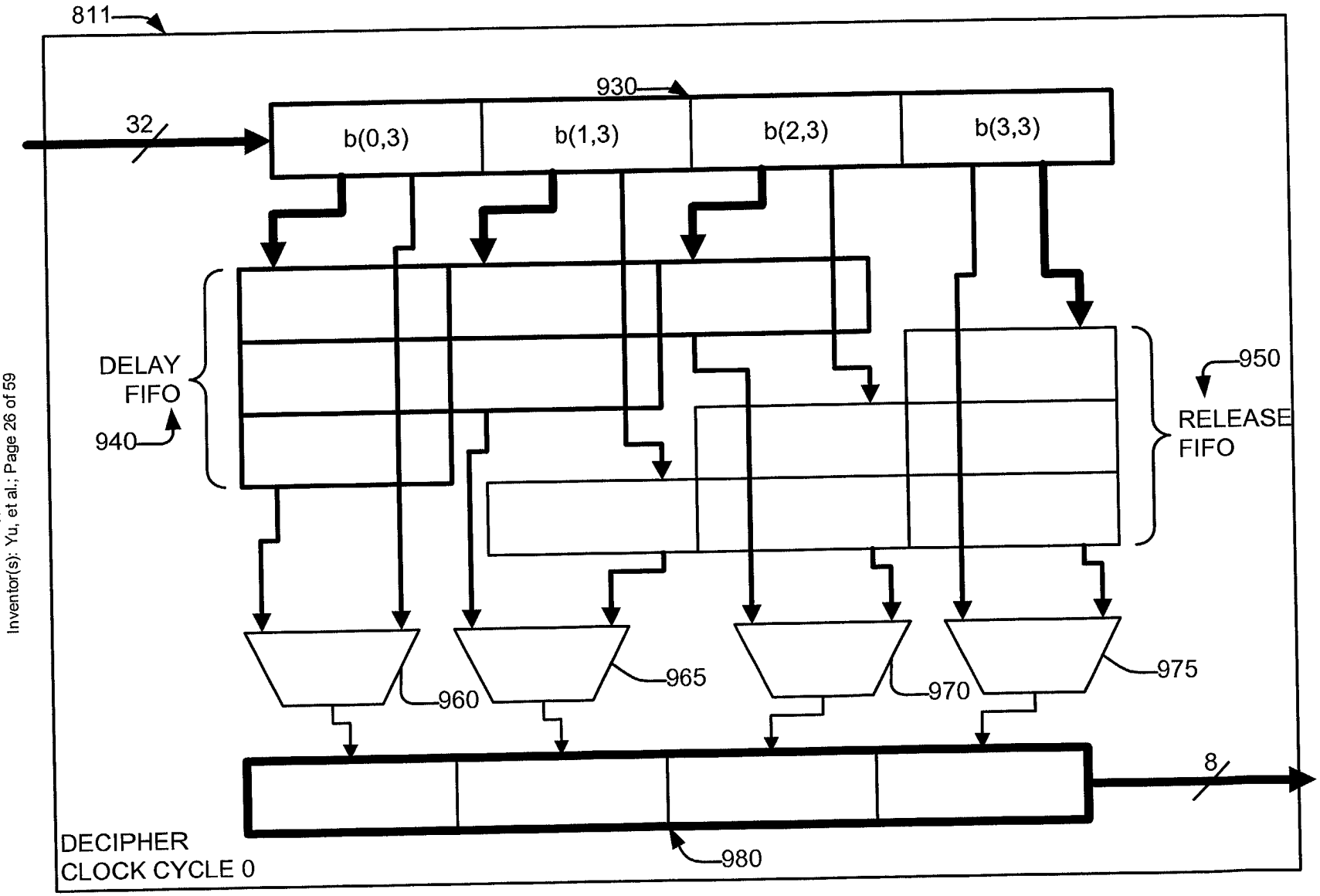

811
930
32
b(0,3)
b(1,3)
b(2,3)
b(3,3)
DELAY
FIFO
940
950
RELEASE
FIFO
960
965
970
975
8
980
DECIPHER
CLOCK CYCLE 0

FIG. 9I

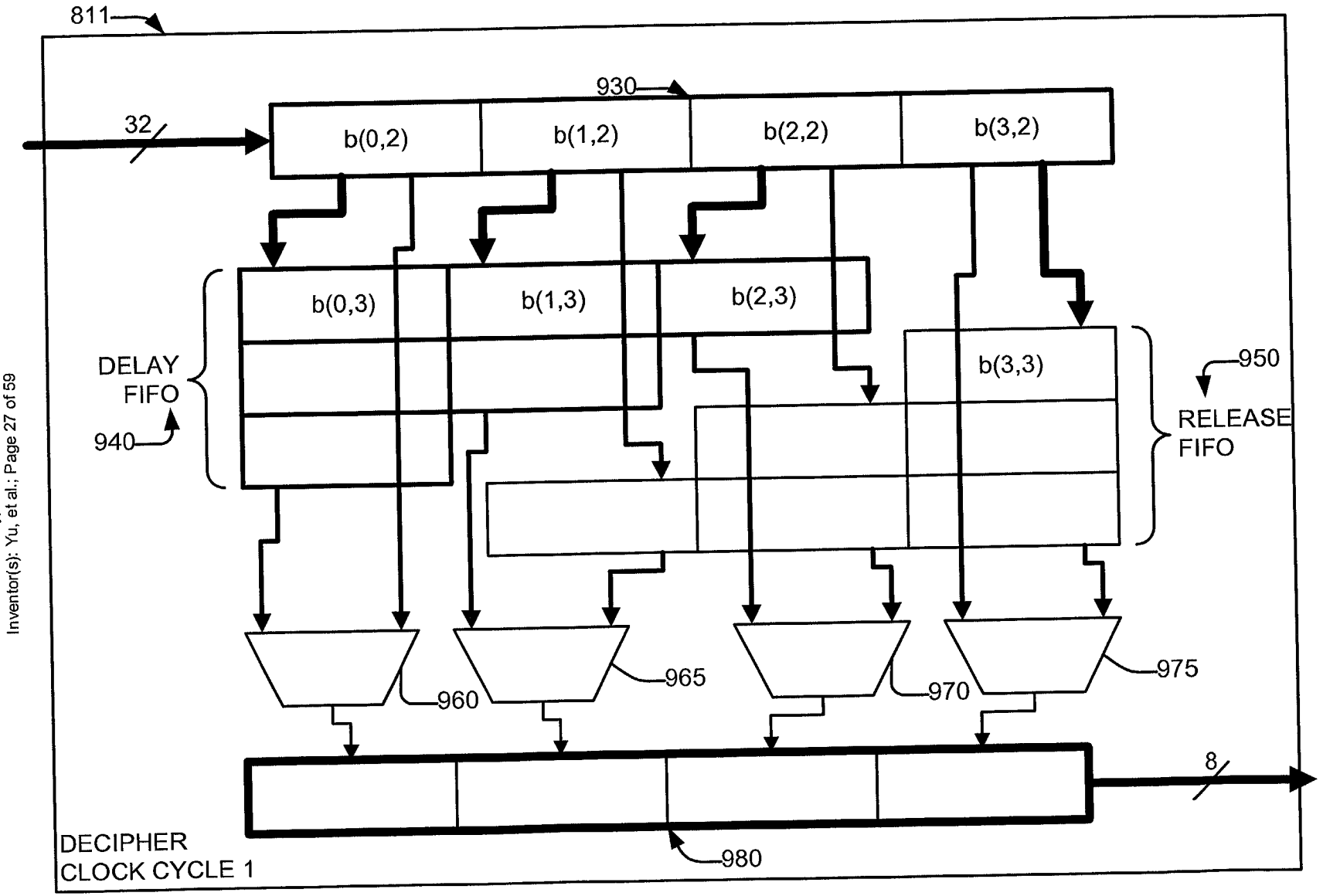

811
930
32
b(0,2)
b(1,2)
b(2,2)
b(3,2)
b(0,3)
b(1,3)
b(2,3)
b(3,3)
DELAY
FIFO
940
950
RELEASE
FIFO
960
965
970
975
8
980
DECIPHER
CLOCK CYCLE 1

FIG. 9J

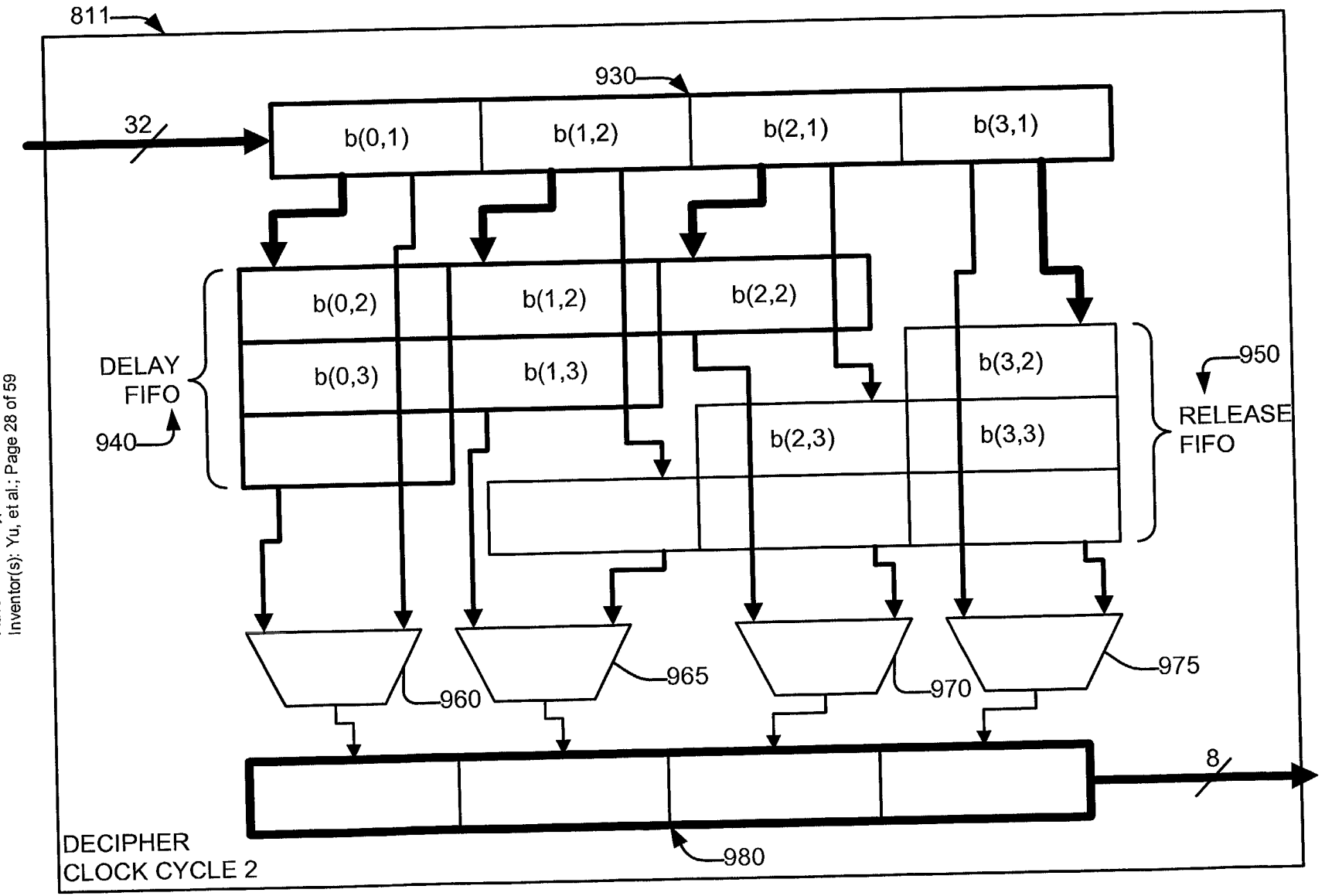

811
930
32
b(0,1)
b(1,2)
b(2,1)
b(3,1)
b(0,2)
b(1,2)
b(2,2)
b(0,3)
b(1,3)
b(2,3)
b(3,2)
b(3,3)
DELAY FIFO
940
950
RELEASE FIFO
960
965
970
975
8
980
DECIPHER
CLOCK CYCLE 2

FIG. 9K

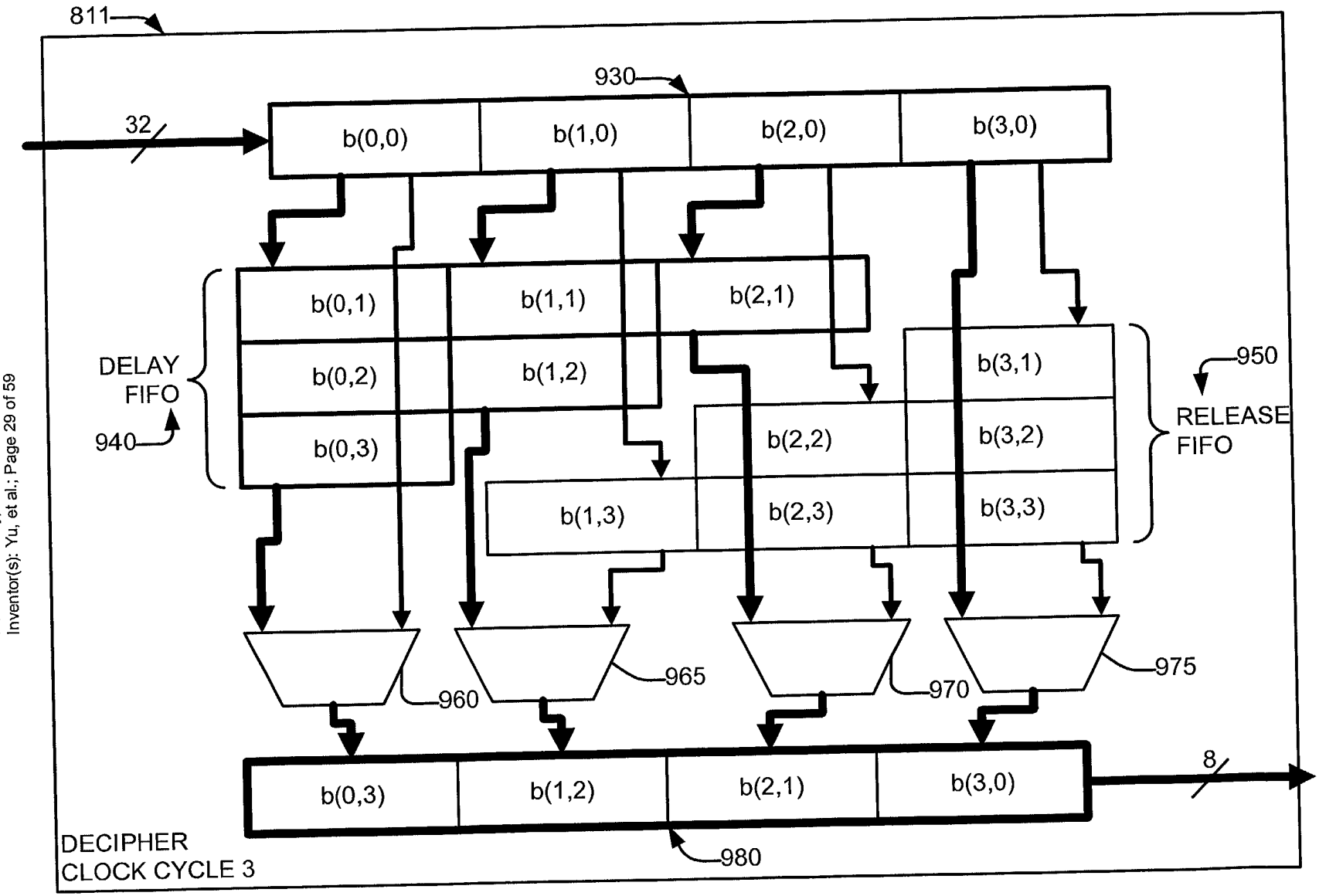

811
930
32
b(0,0)
b(1,0)
b(2,0)
b(3,0)
b(0,1)
b(1,1)
b(2,1)
b(3,1)
DELAY
FIFO
940
b(0,2)
b(1,2)
b(2,2)
b(3,2)
950
RELEASE
FIFO
b(0,3)
b(1,3)
b(2,3)
b(3,3)
960
965
970
975
8
b(0,3)
b(1,2)
b(2,1)
b(3,0)
980
DECIPHER
CLOCK CYCLE 3

FIG. 9L

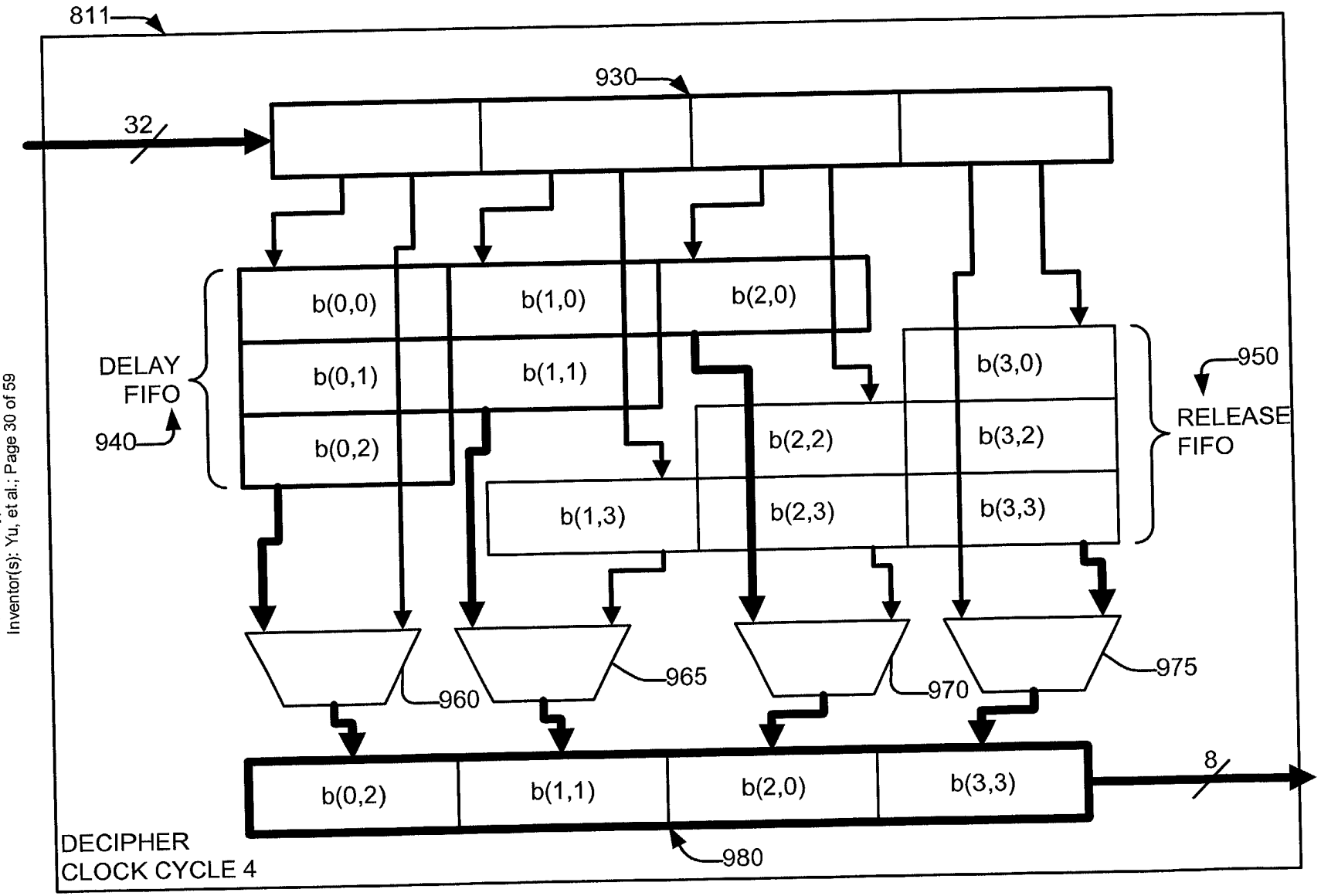

811
930
32
b(0,0)
b(1,0)
b(2,0)
b(0,1)
b(1,1)
b(0,2)
b(2,2)
b(3,0)
b(3,2)
b(1,3)
b(2,3)
b(3,3)
DELAY FIFO
940
950
RELEASE FIFO
960
965
970
975
8
b(0,2)
b(1,1)
b(2,0)
b(3,3)
980
DECIPHER
CLOCK CYCLE 4

FIG. 9M

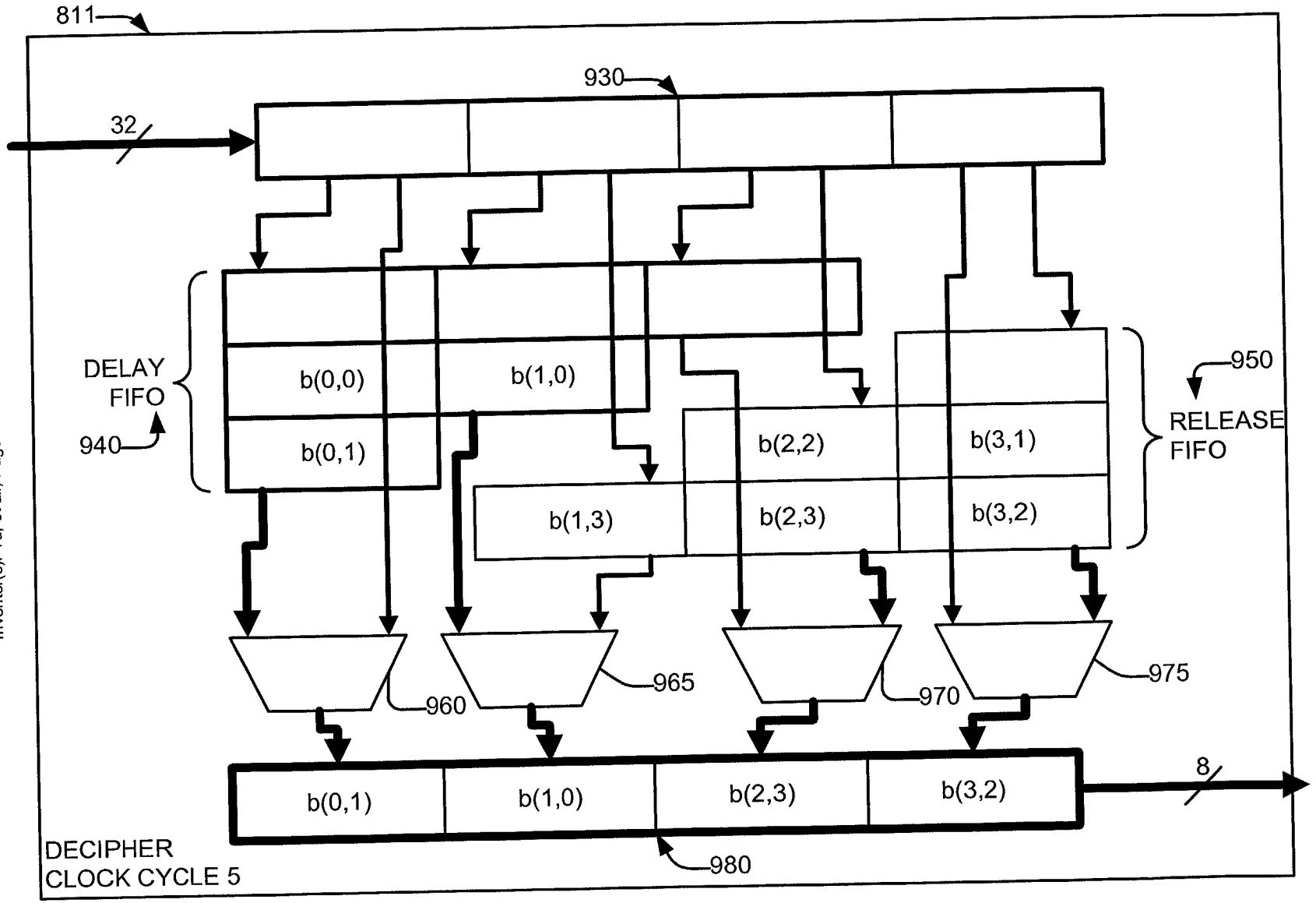

811
930
32
DELAY
FIFO
940
b(0,0)
b(1,0)
b(0,1)
b(2,2)
b(3,1)
b(1,3)
b(2,3)
b(3,2)
950
RELEASE
FIFO
960
965
970
975
b(0,1)
b(1,0)
b(2,3)
b(3,2)
8
980
DECIPHER
CLOCK CYCLE 5

FIG. 9N

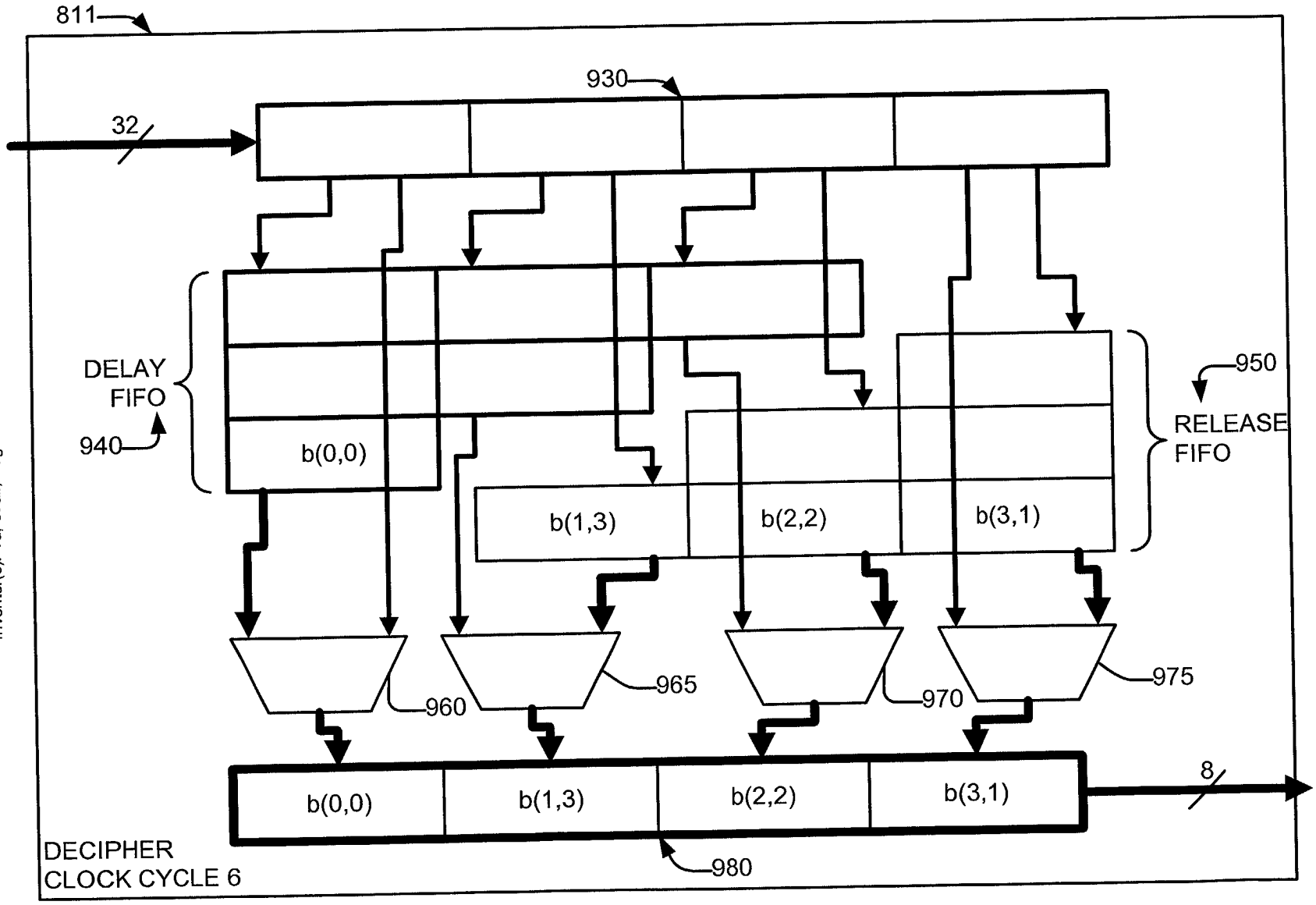

811
930
32
DELAY
FIFO
940
b(0,0)
950
RELEASE
FIFO
b(1,3)
b(2,2)
b(3,1)
960
965
970
975
8
b(0,0)
b(1,3)
b(2,2)
b(3,1)
980
DECIPHER
CLOCK CYCLE 6

FIG. 9O

20020 01980T

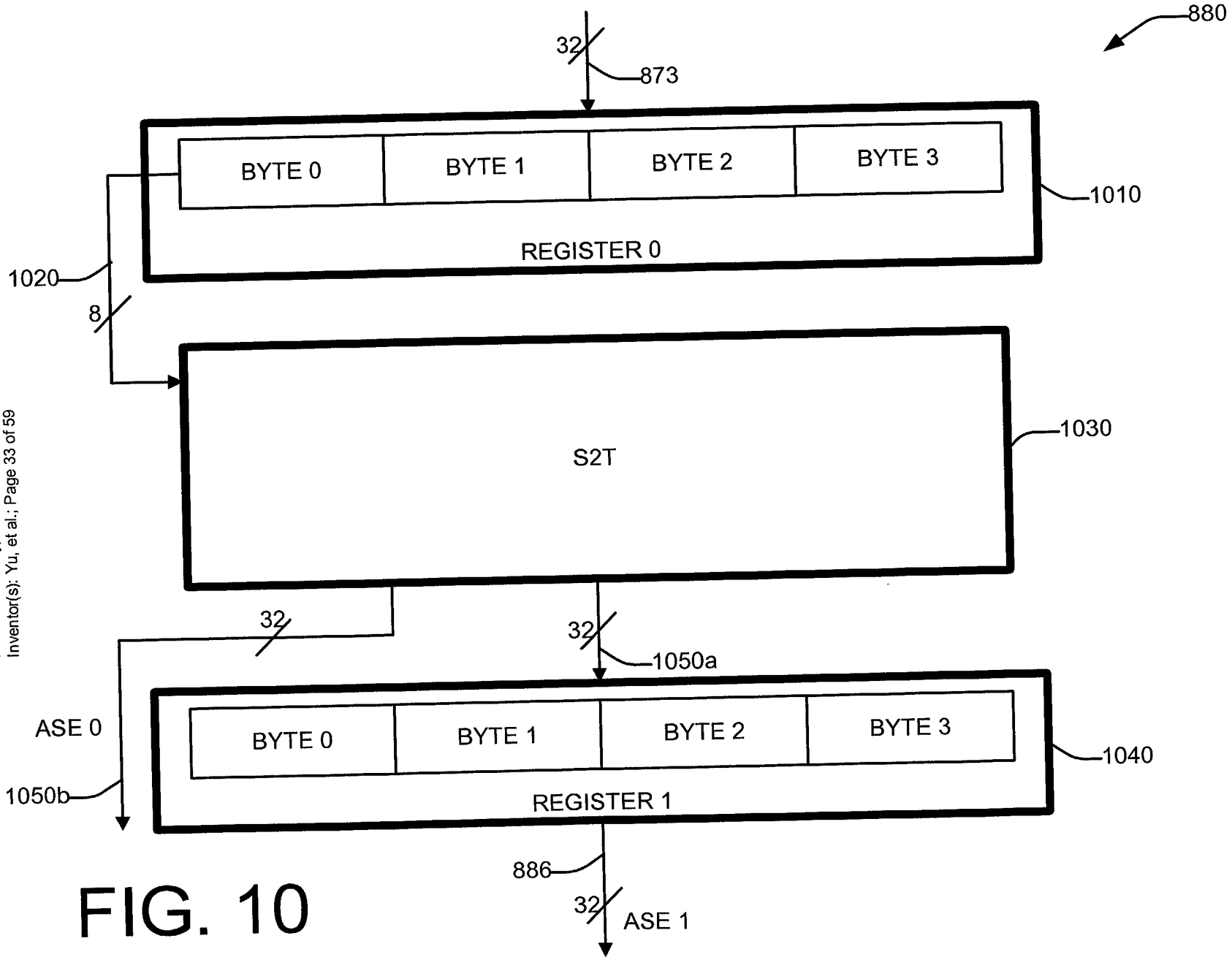


FIG. 10

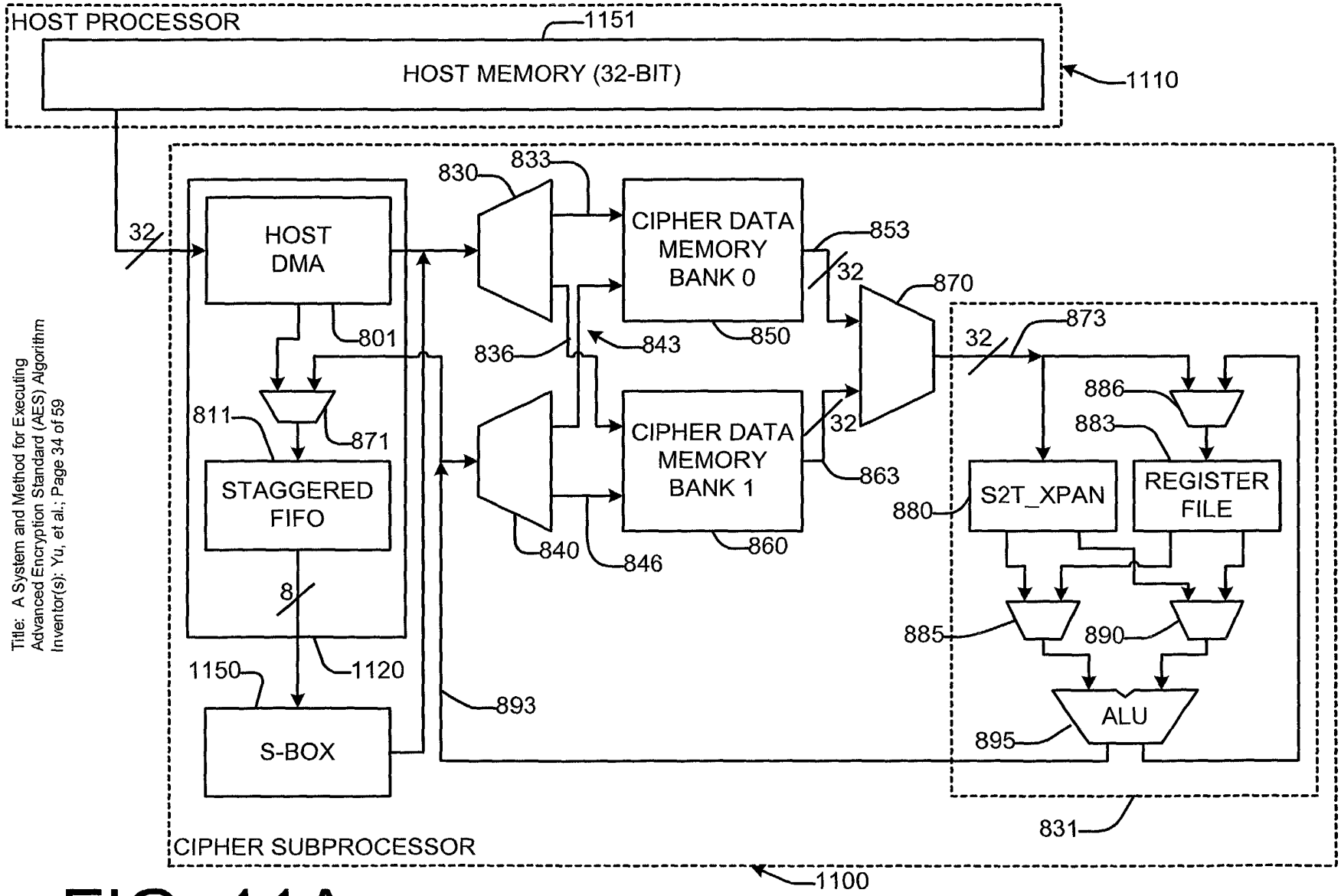


FIG. 11A

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 34 of 59

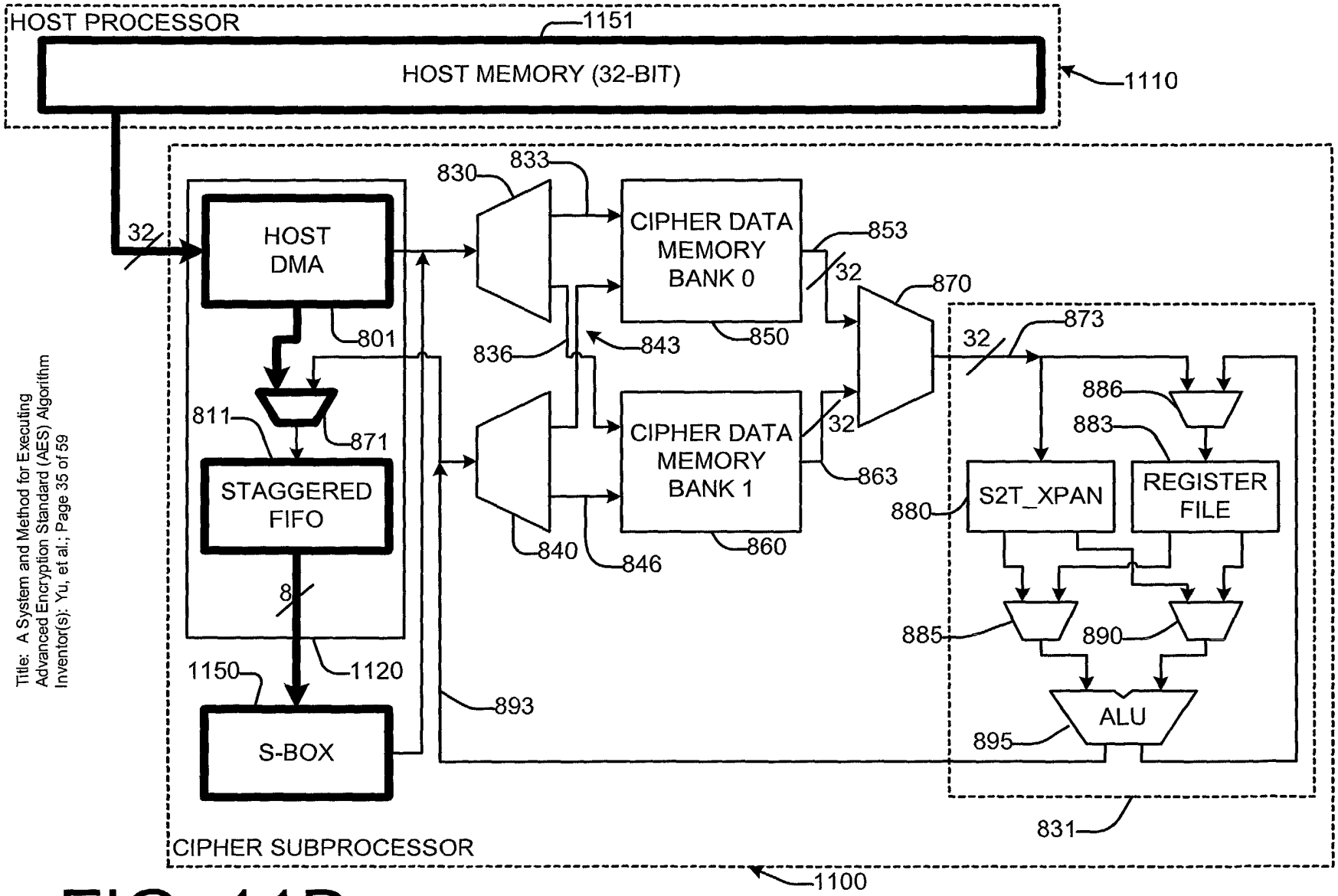


FIG. 11B

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 35 of 59

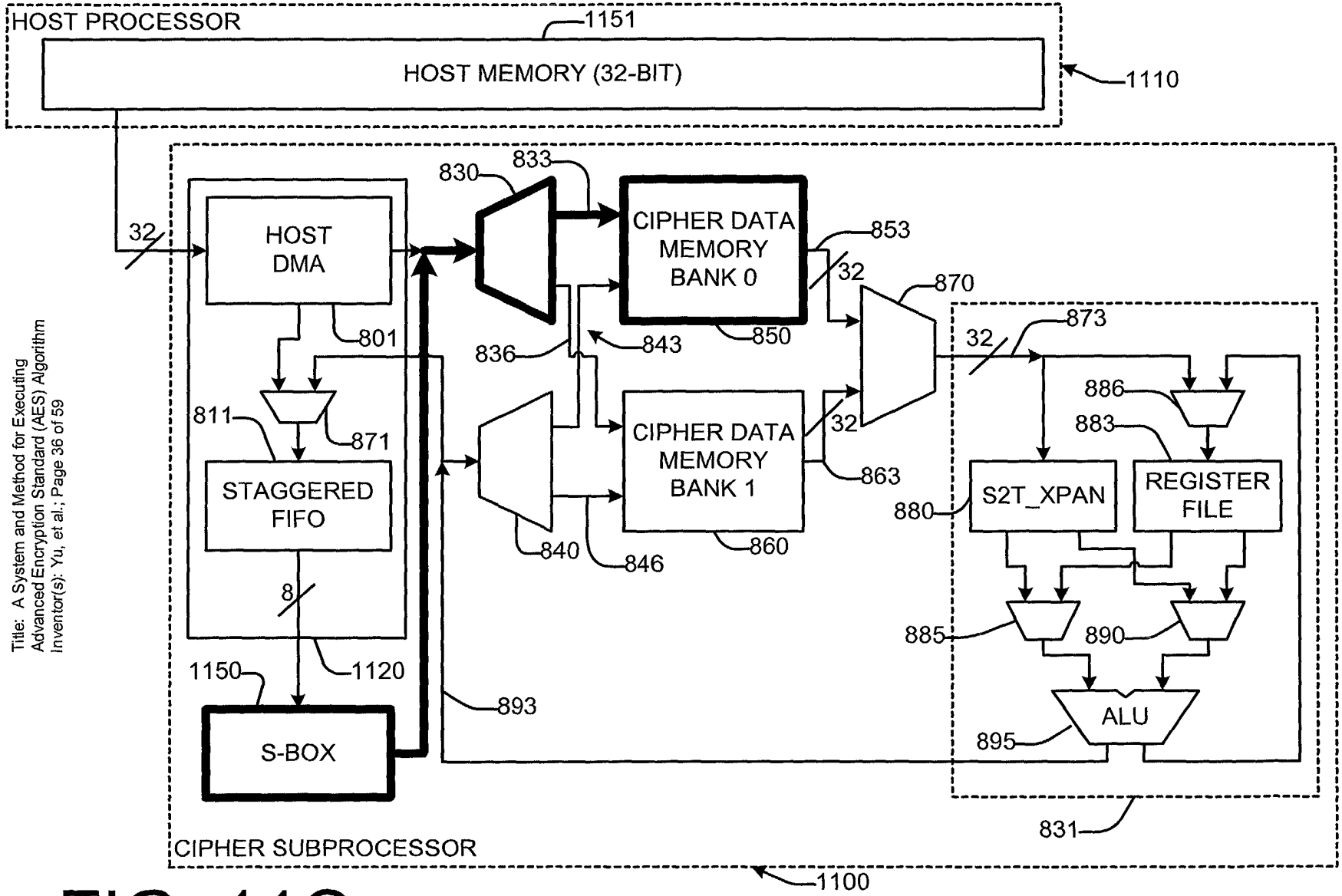


FIG. 11C

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 36 of 59

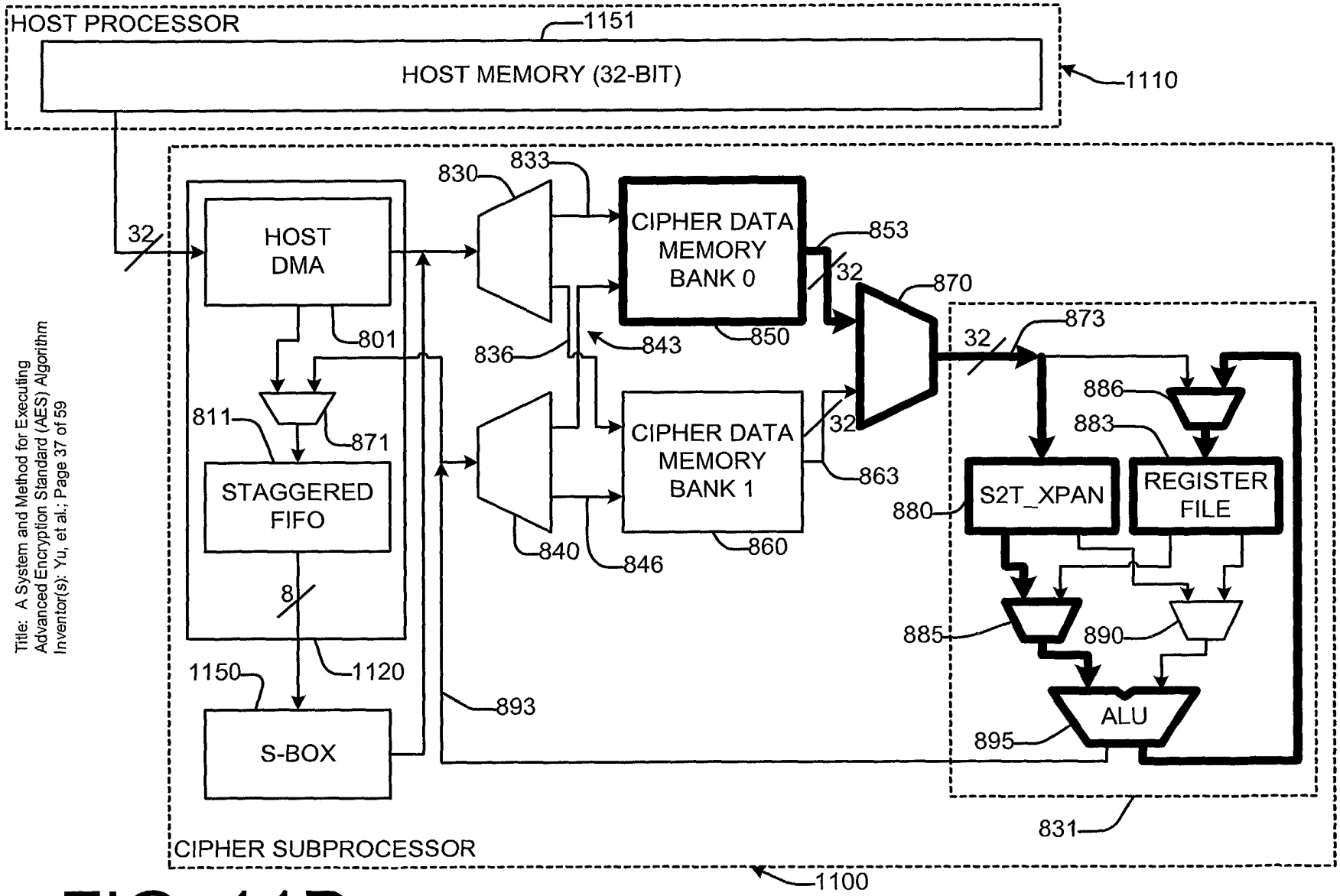


FIG. 11D

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 37 of 59

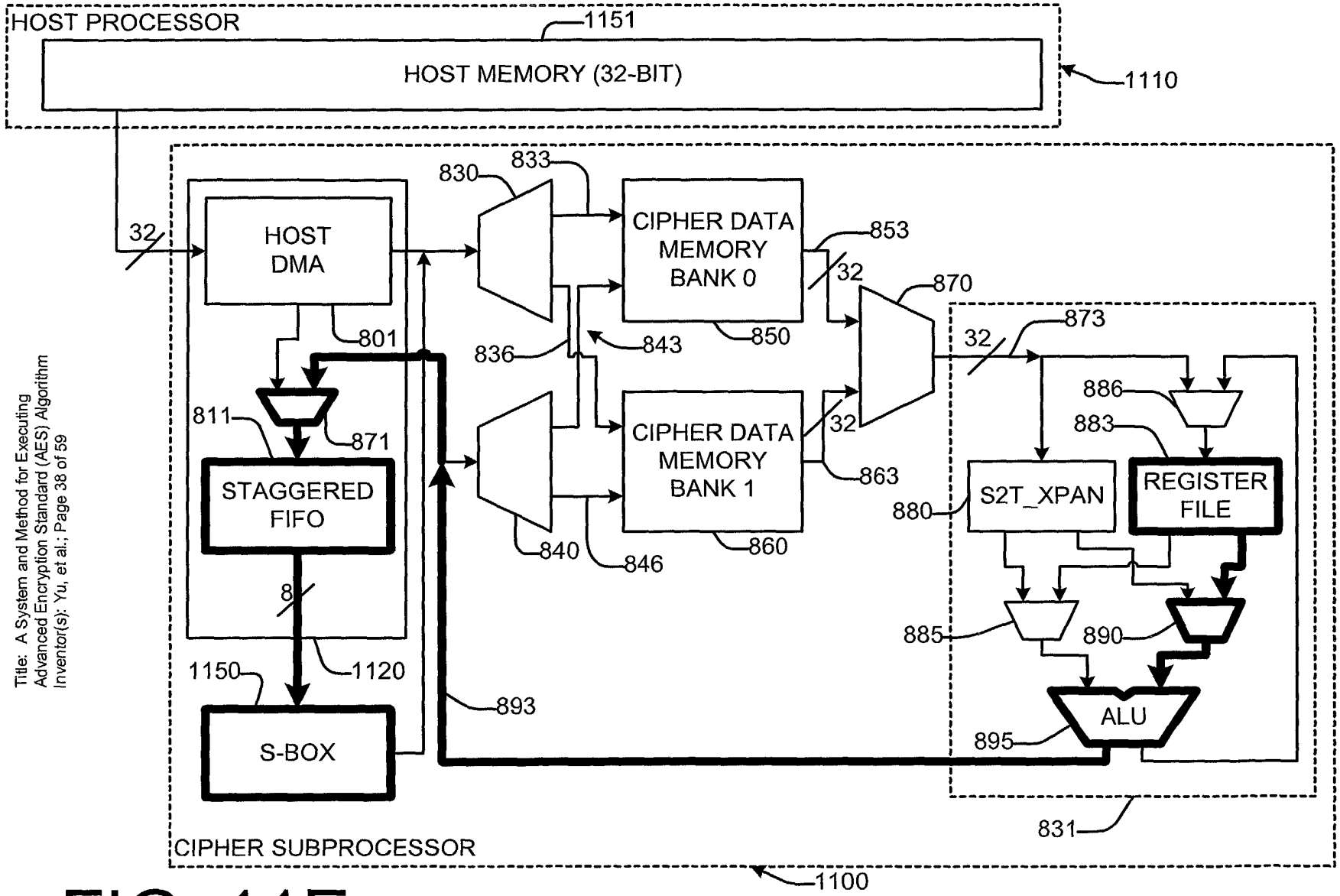


FIG. 11E

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 38 of 59

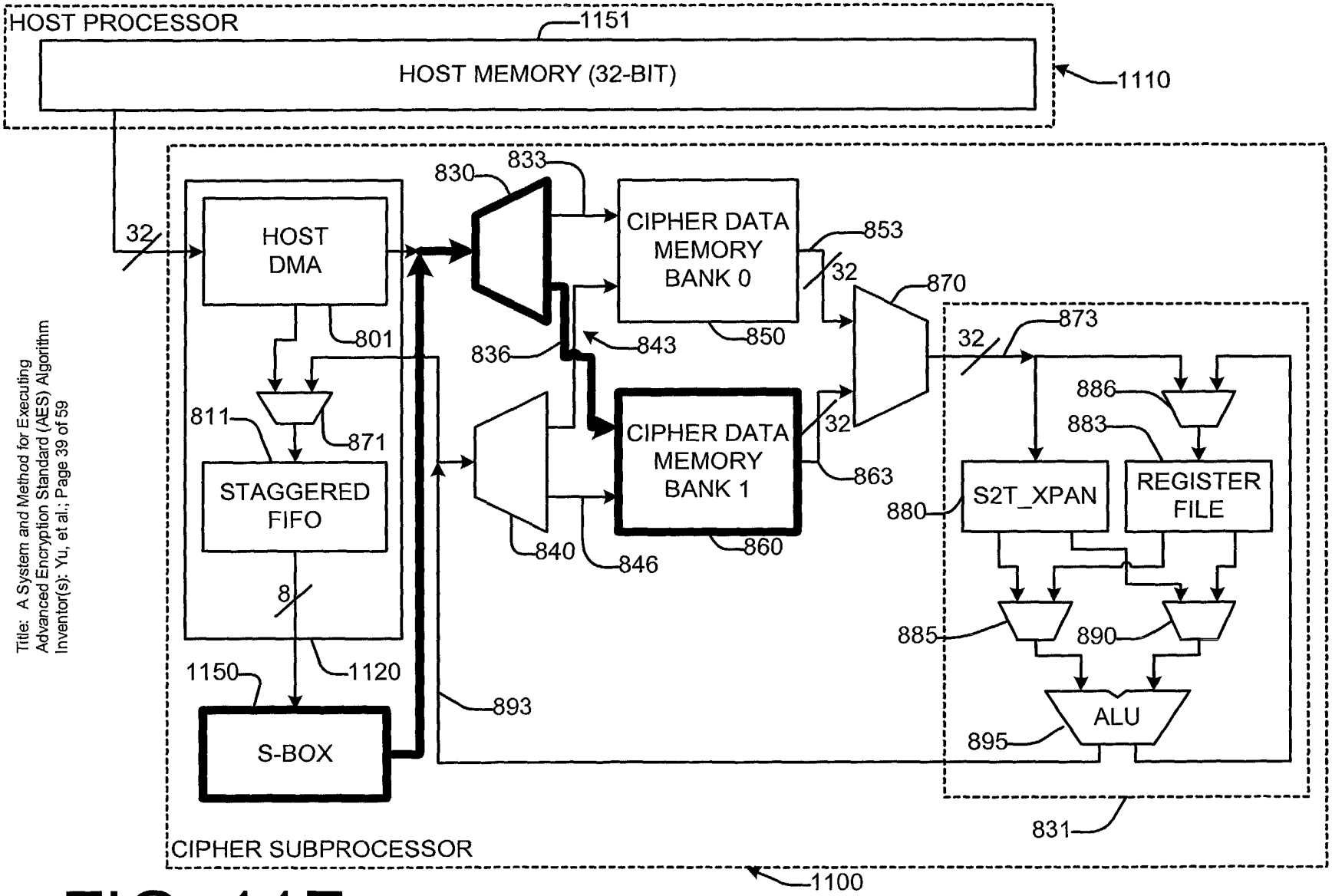


FIG. 11F

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 39 of 59

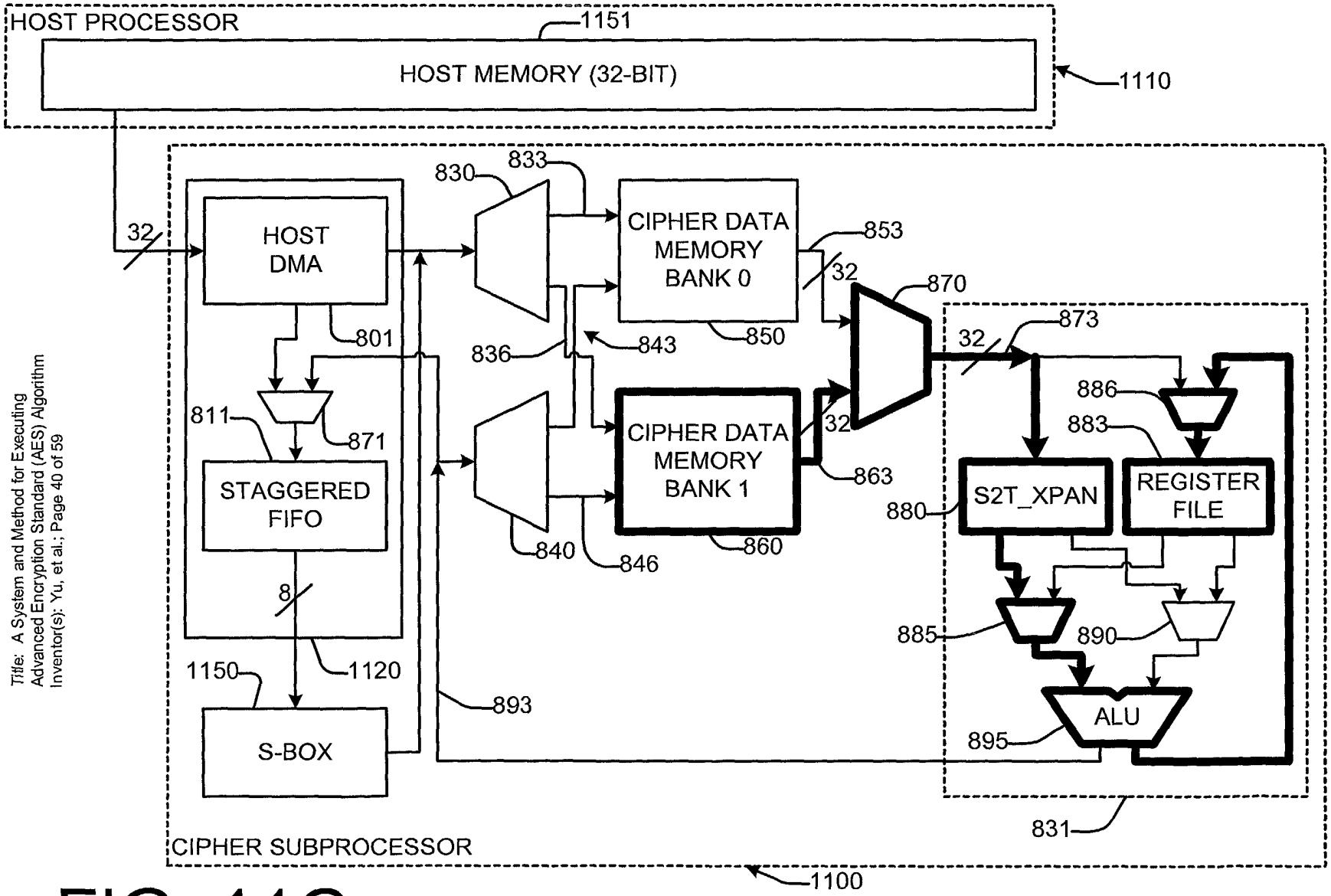


FIG. 11G

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 40 of 59

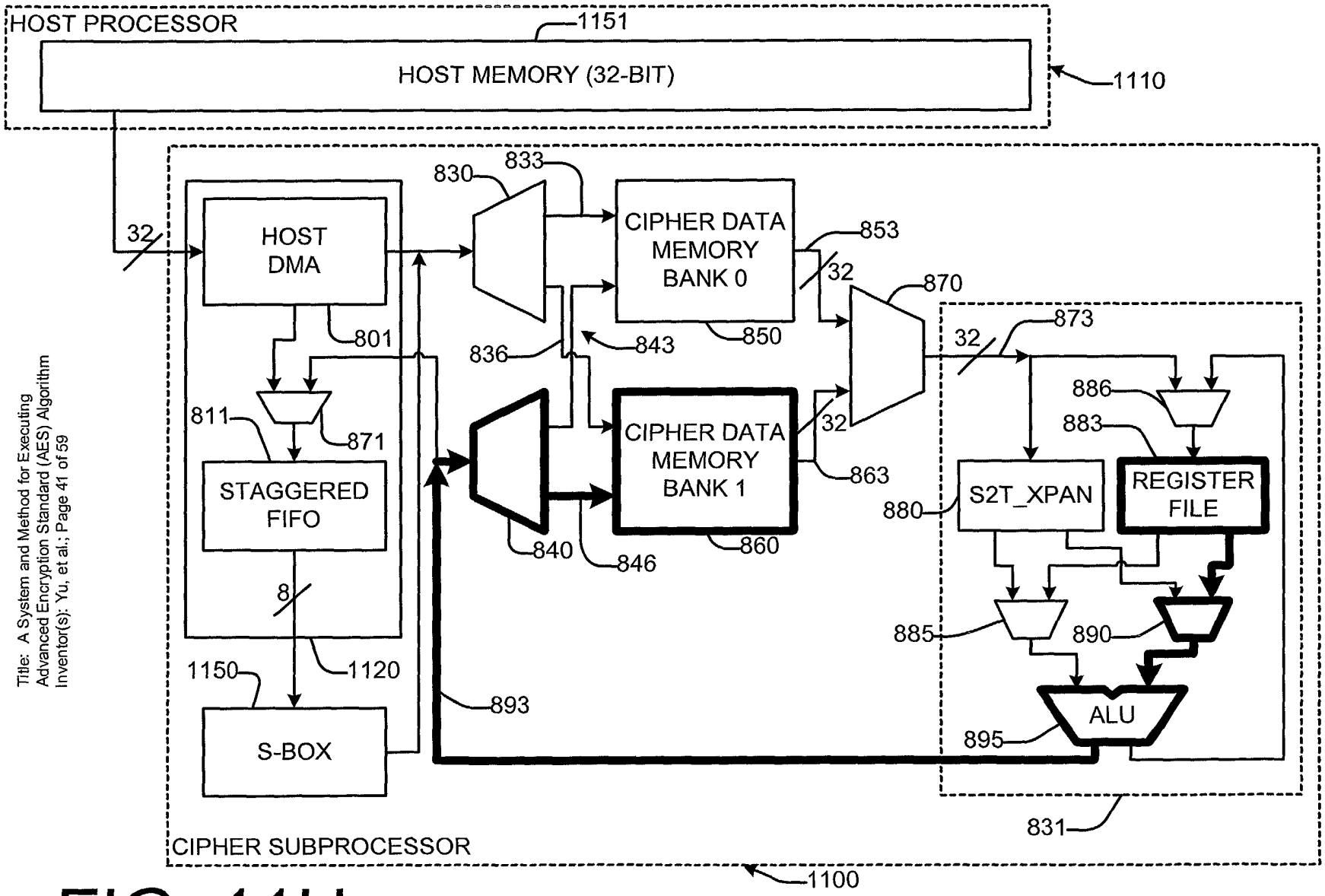


FIG. 11H

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 41 of 59

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 42 of 59

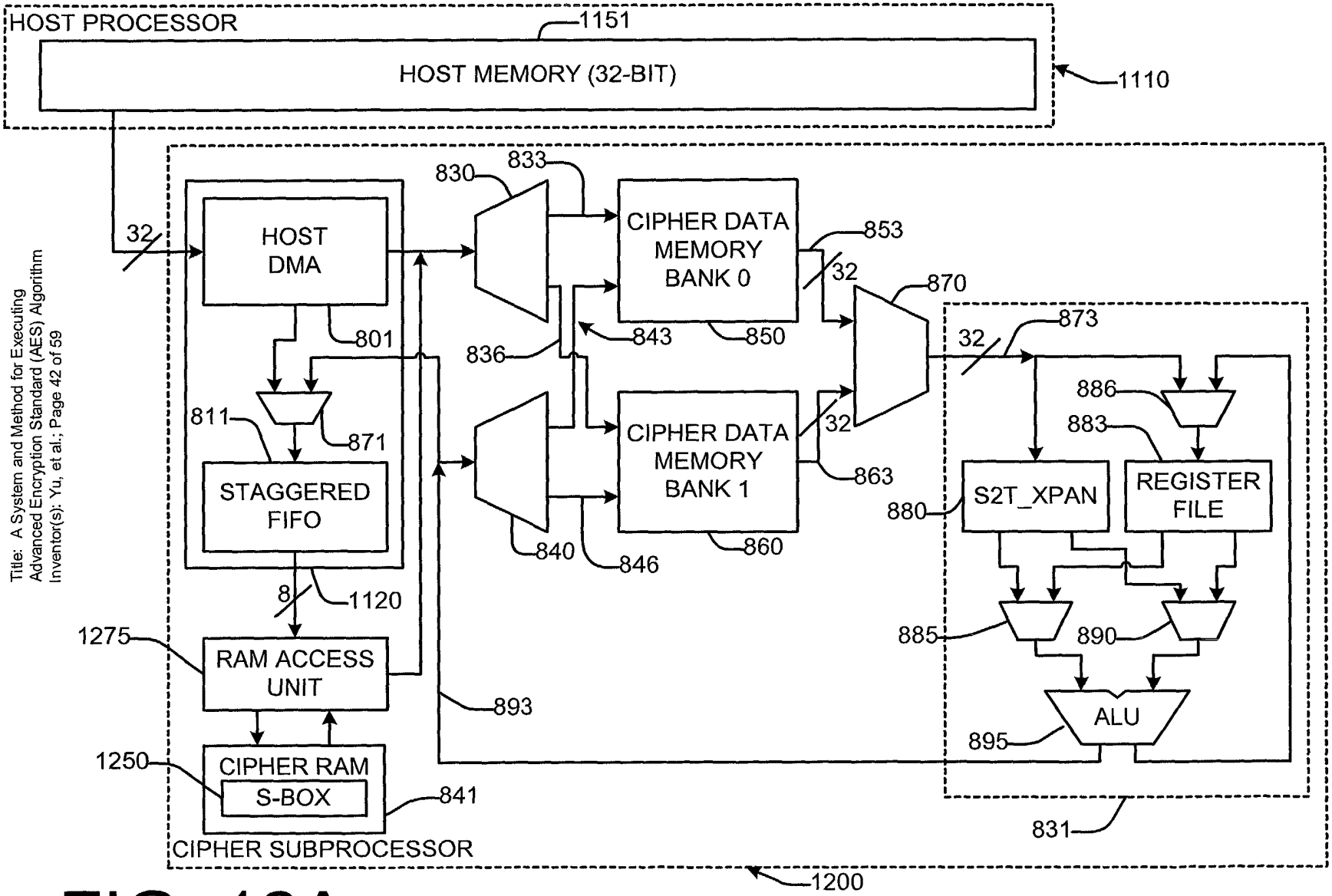
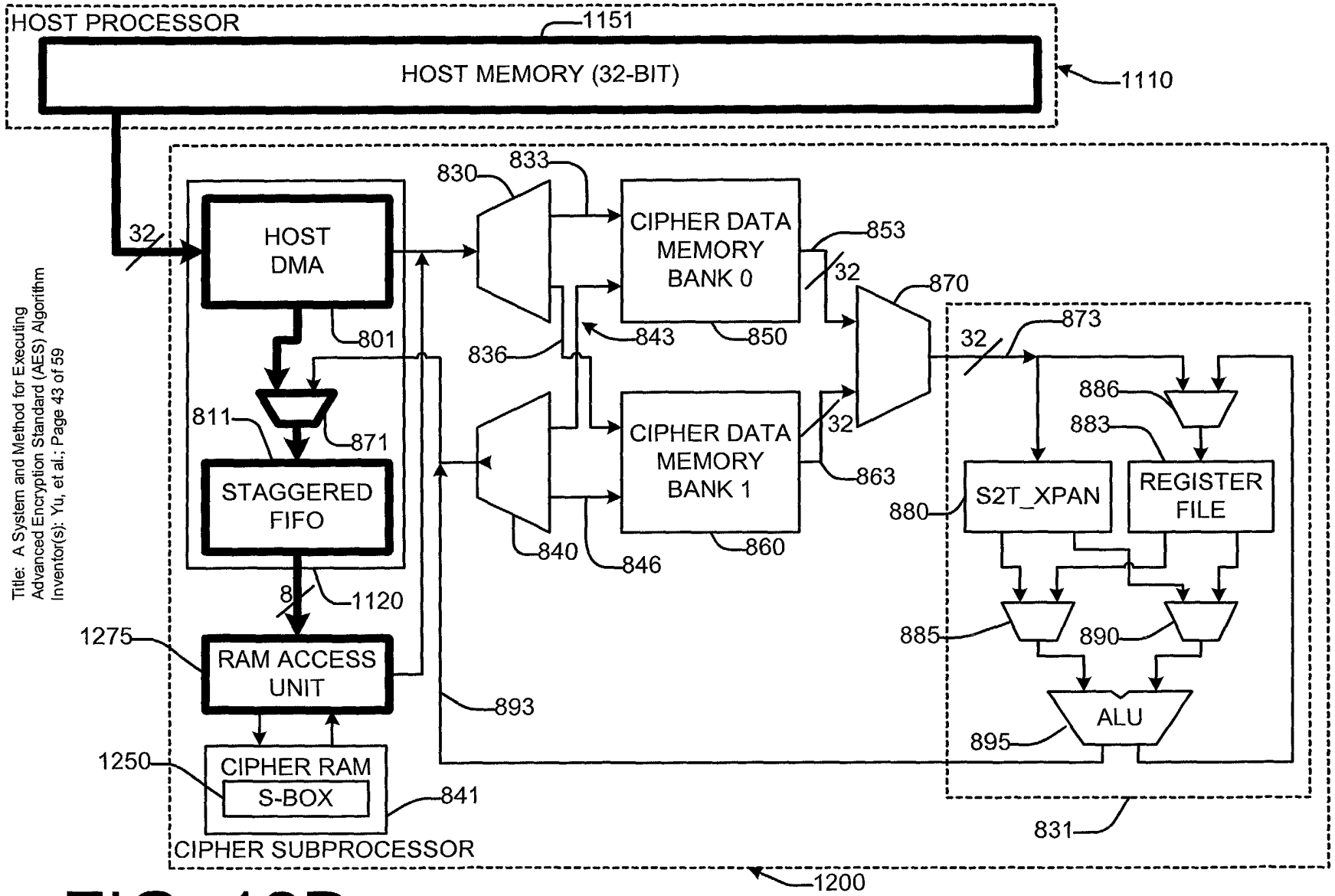


FIG. 12A



Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 43 of 59

FIG. 12B

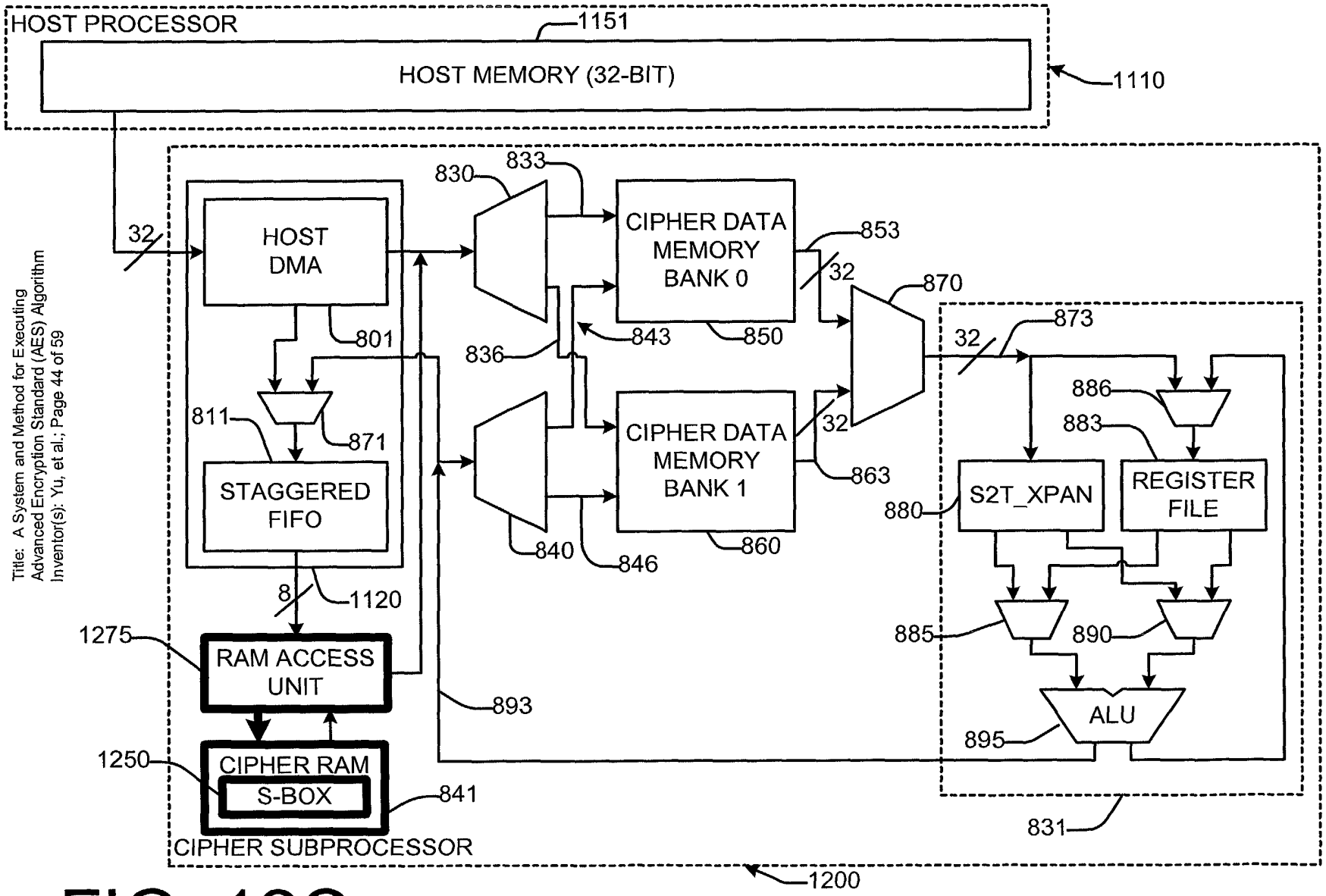


FIG. 12C

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 44 of 59

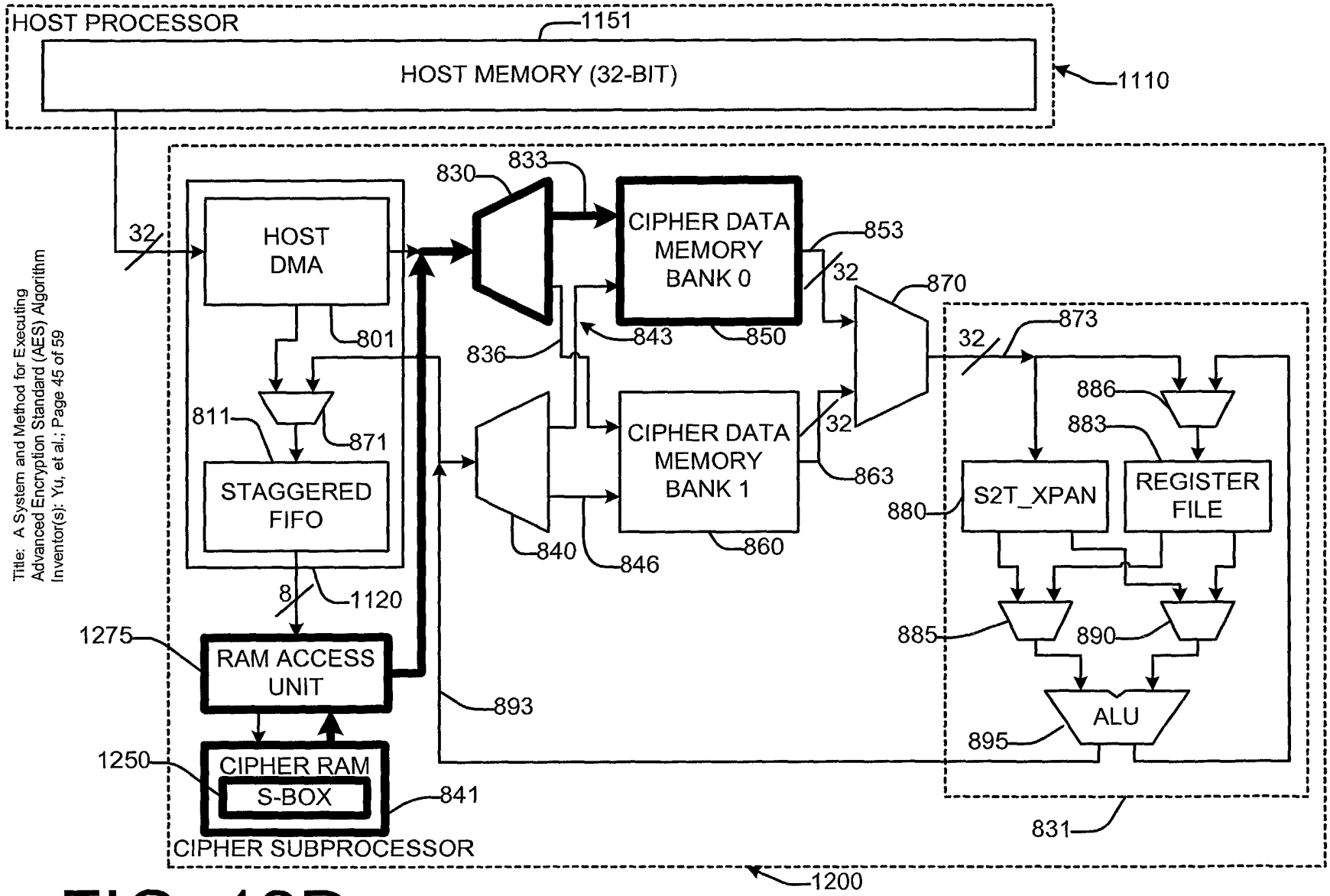


FIG. 12D

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 45 of 59

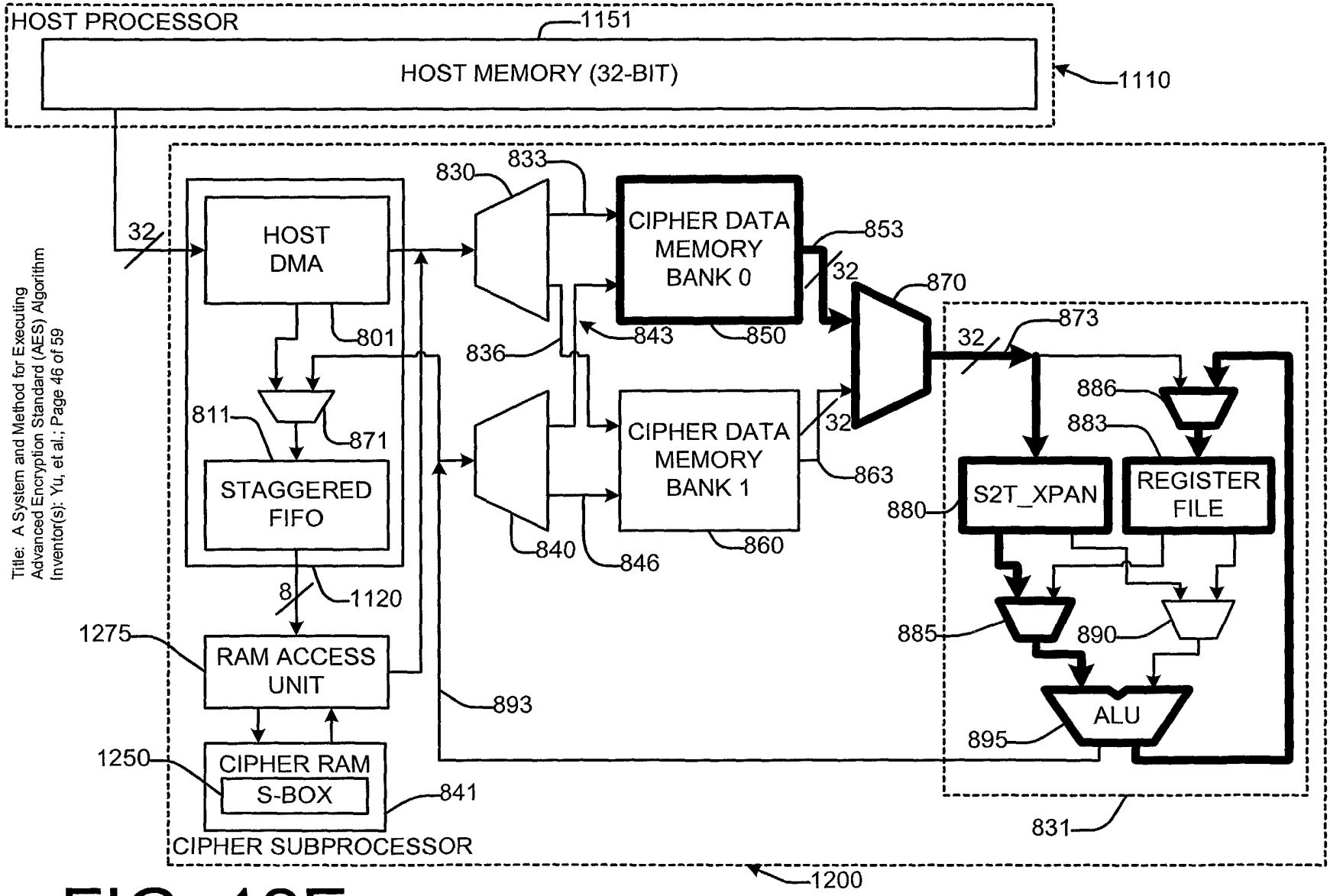


FIG. 12E

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 46 of 59

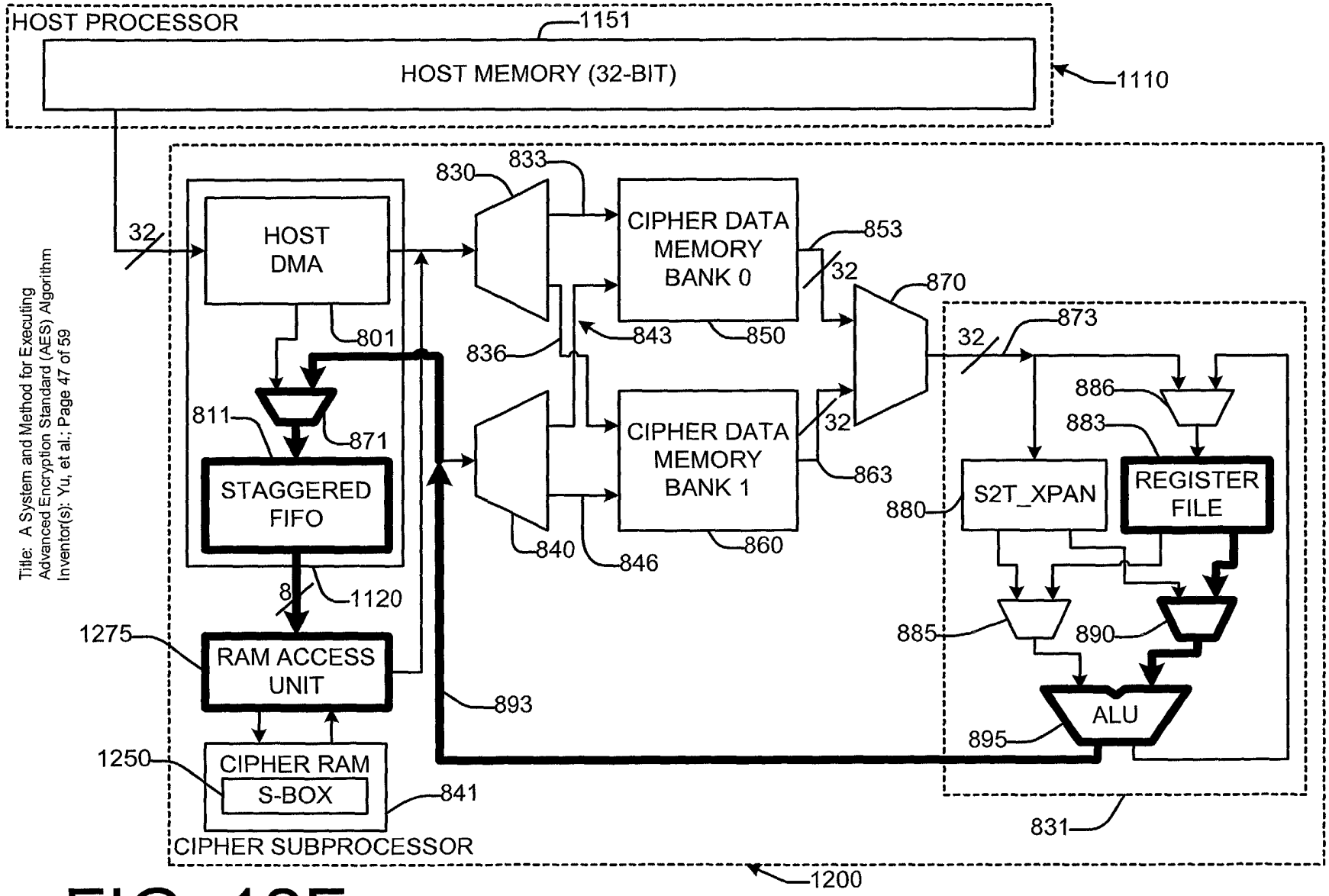


FIG. 12F

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 47 of 59

20030 "0T98900T

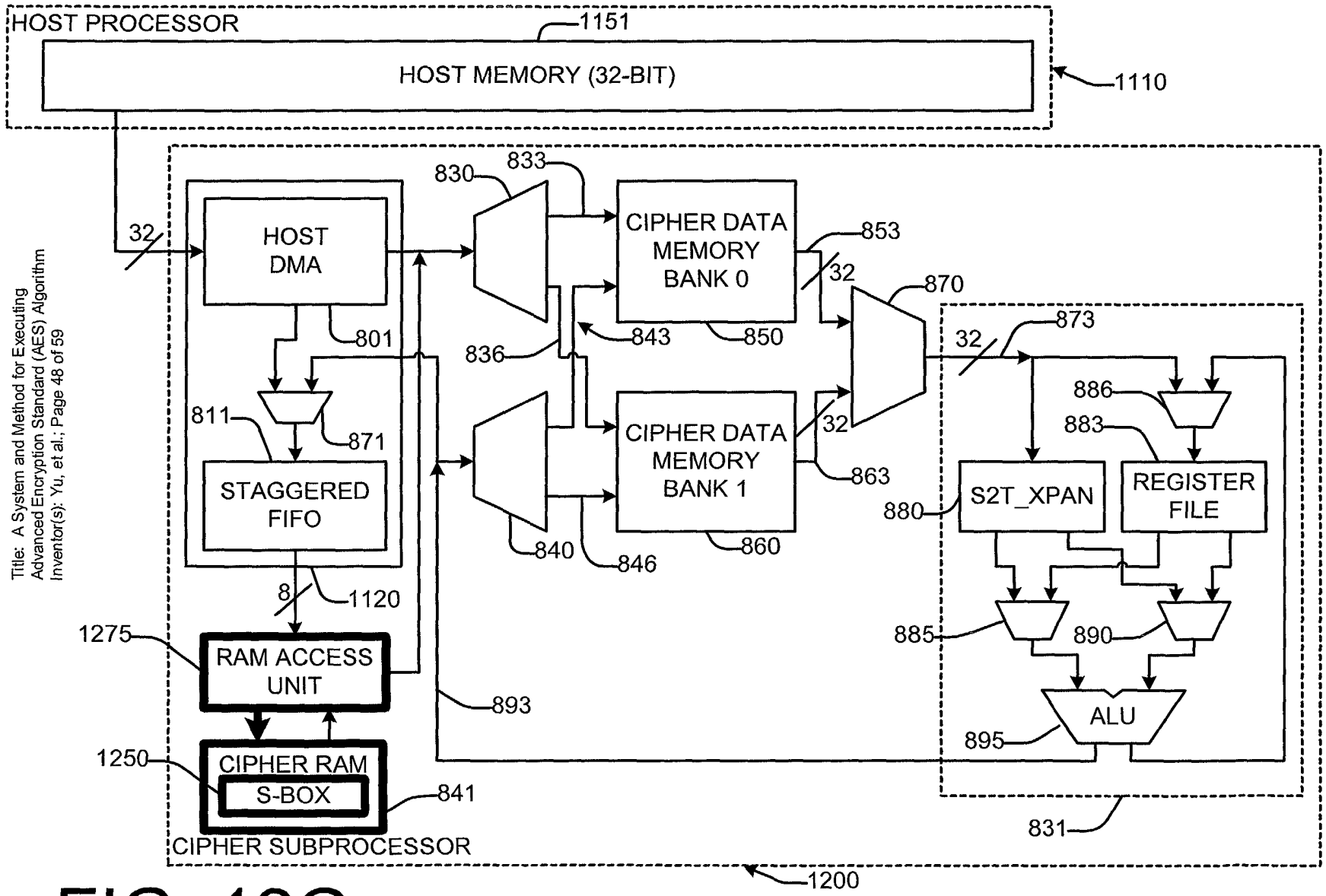
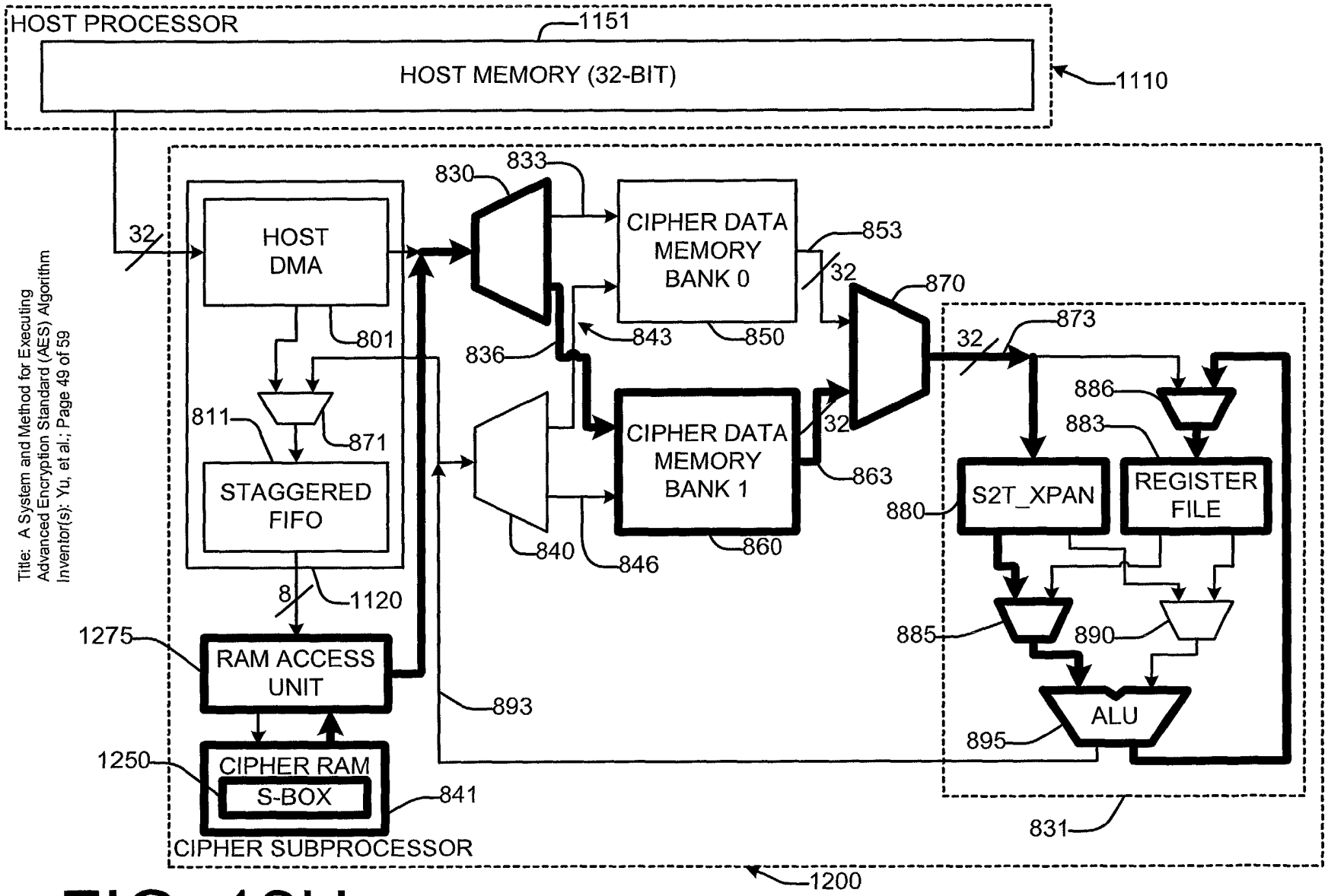


FIG. 12G

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 48 of 59



Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 49 of 59

FIG. 12H

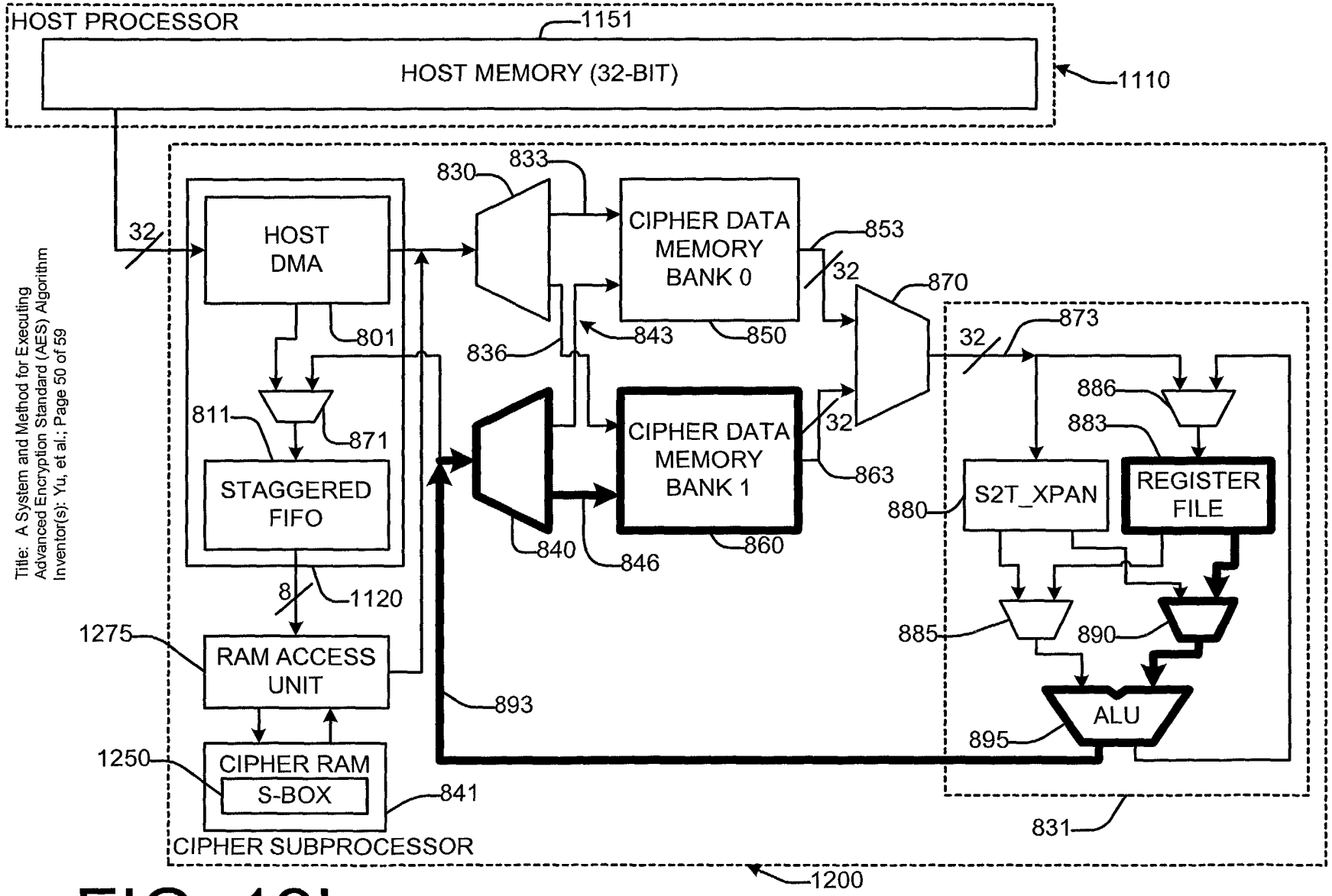


FIG. 12I

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 50 of 59

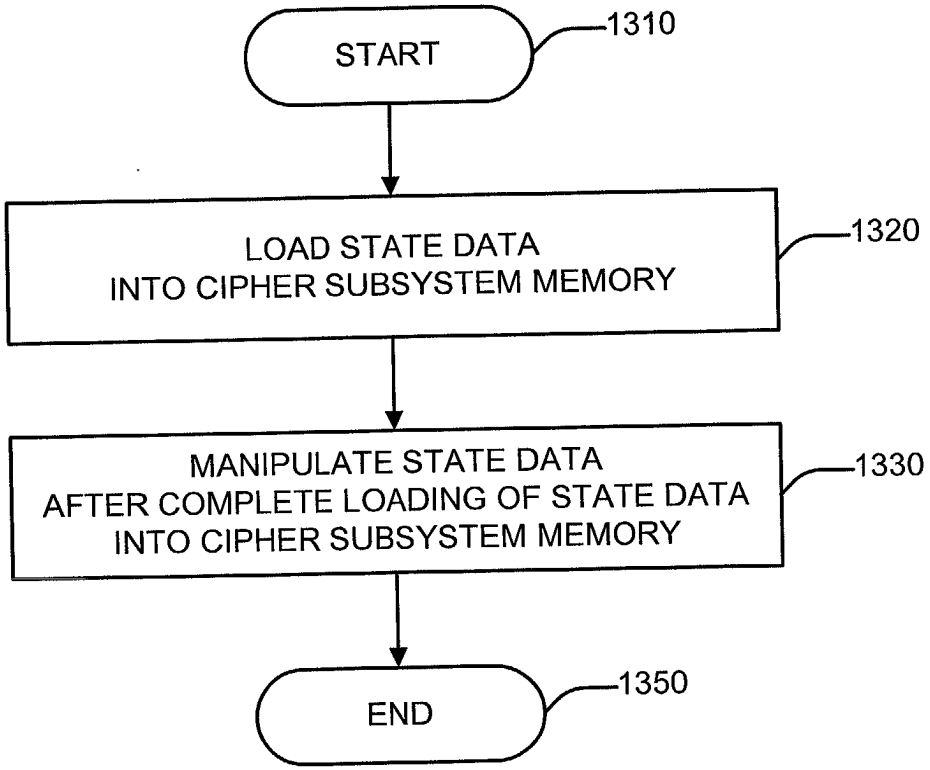


FIG. 13
(PRIOR ART)

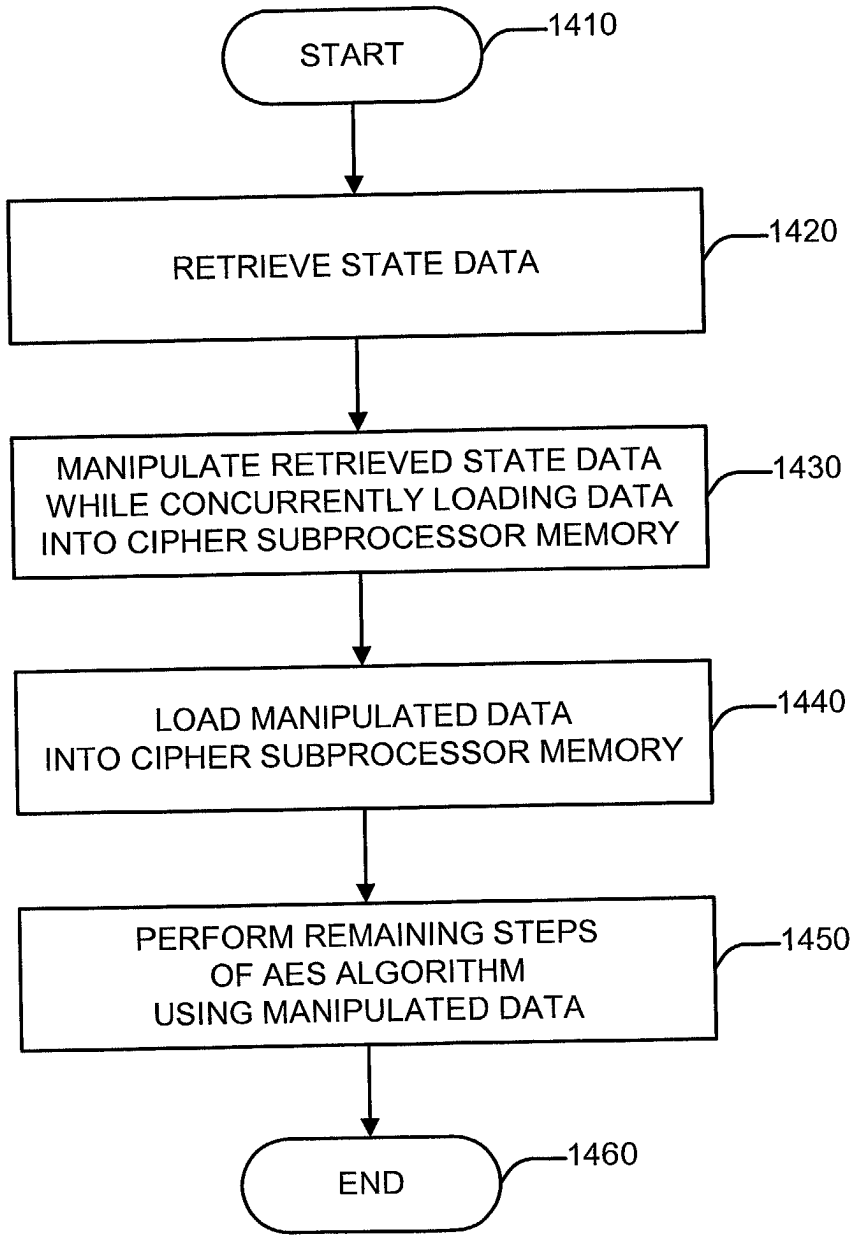

START
1410
RETRIEVE STATE DATA
1420
MANIPULATE RETRIEVED STATE DATA
WHILE CONCURRENTLY LOADING DATA
INTO CIPHER SUBPROCESSOR MEMORY
1430
LOAD MANIPULATED DATA
INTO CIPHER SUBPROCESSOR MEMORY
1440
PERFORM REMAINING STEPS
OF AES ALGORITHM
USING MANIPULATED DATA
1450
END
1460

FIG. 14

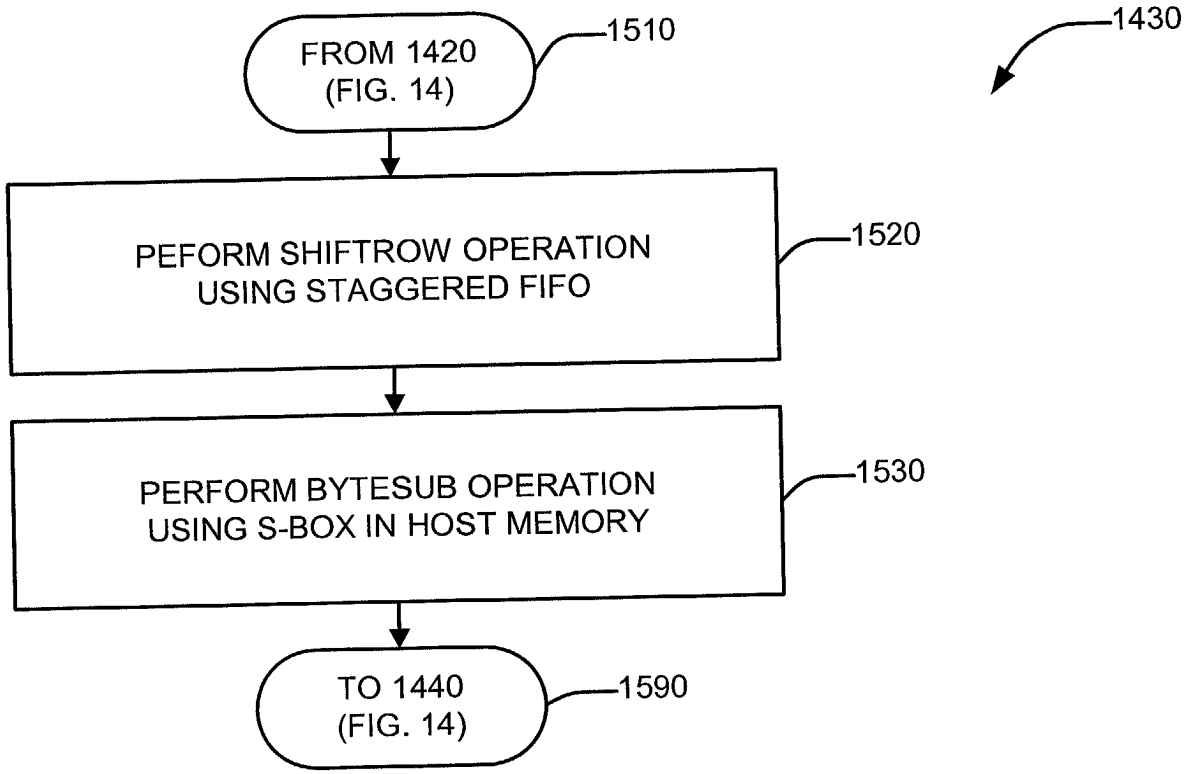

FROM 1420
(FIG. 14)
1510
1430
PEFORM SHIFTROW OPERATION
USING STAGGERED FIFO
1520
PERFORM BYTESUB OPERATION
USING S-BOX IN HOST MEMORY
1530
TO 1440
(FIG. 14)
1590

FIG. 15A

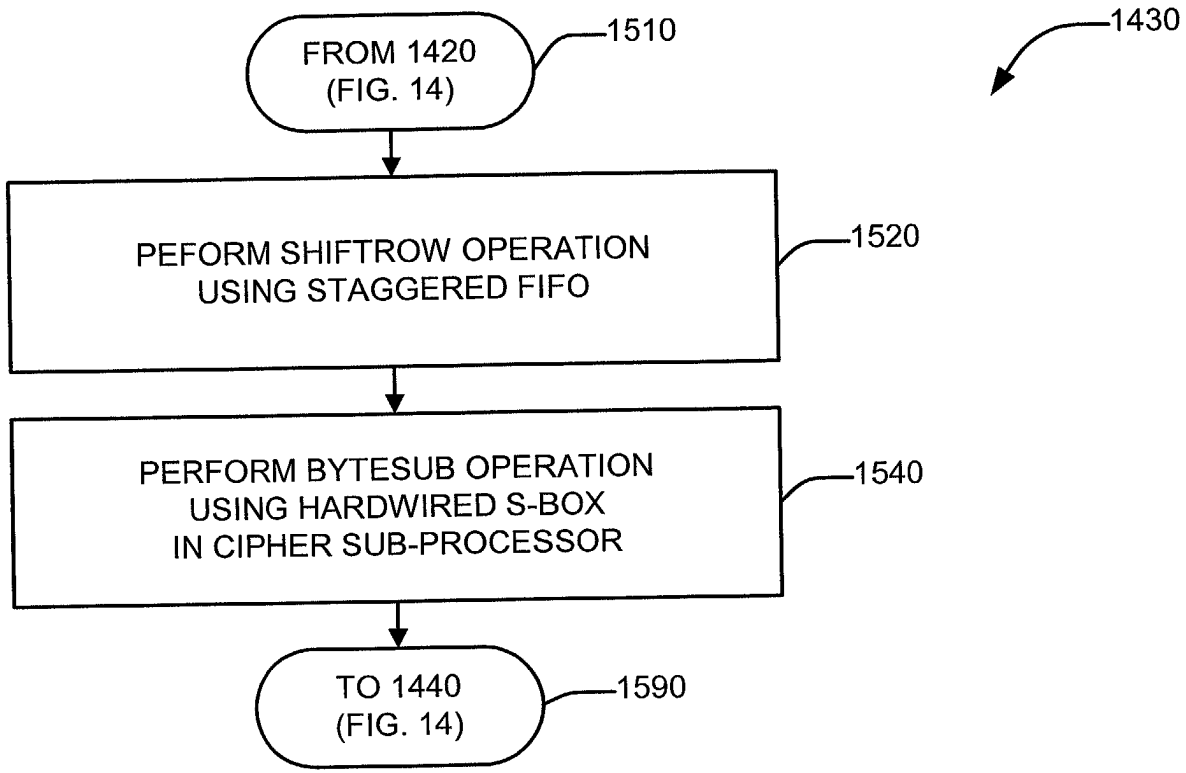

FROM 1420
(FIG. 14)
1510
1430
PEFORM SHIFTROW OPERATION
USING STAGGERED FIFO
1520
PERFORM BYTESUB OPERATION
USING HARDWIRED S-BOX
IN CIPHER SUB-PROCESSOR
1540
TO 1440
(FIG. 14)
1590

FIG. 15B

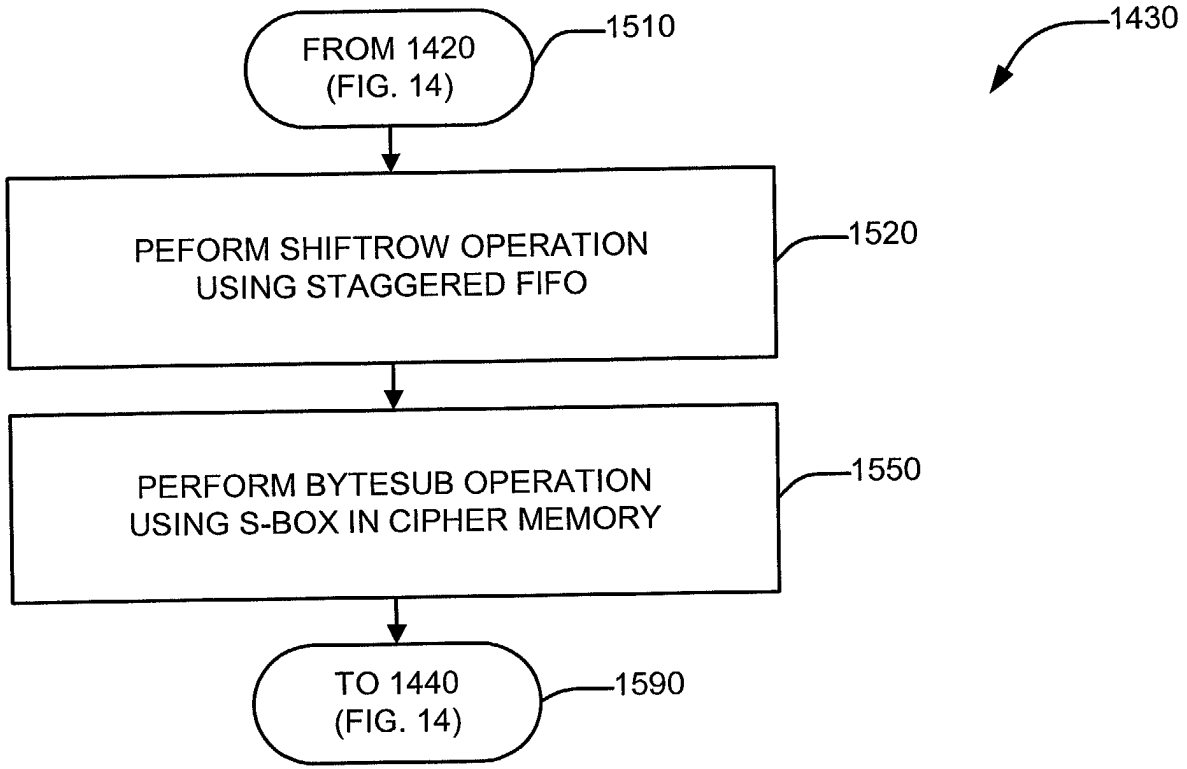

FROM 1420
(FIG. 14)
1510
1430
PEFORM SHIFTROW OPERATION
USING STAGGERED FIFO
1520
PERFORM BYTESUB OPERATION
USING S-BOX IN CIPHER MEMORY
1550
TO 1440
(FIG. 14)
1590

FIG. 15C

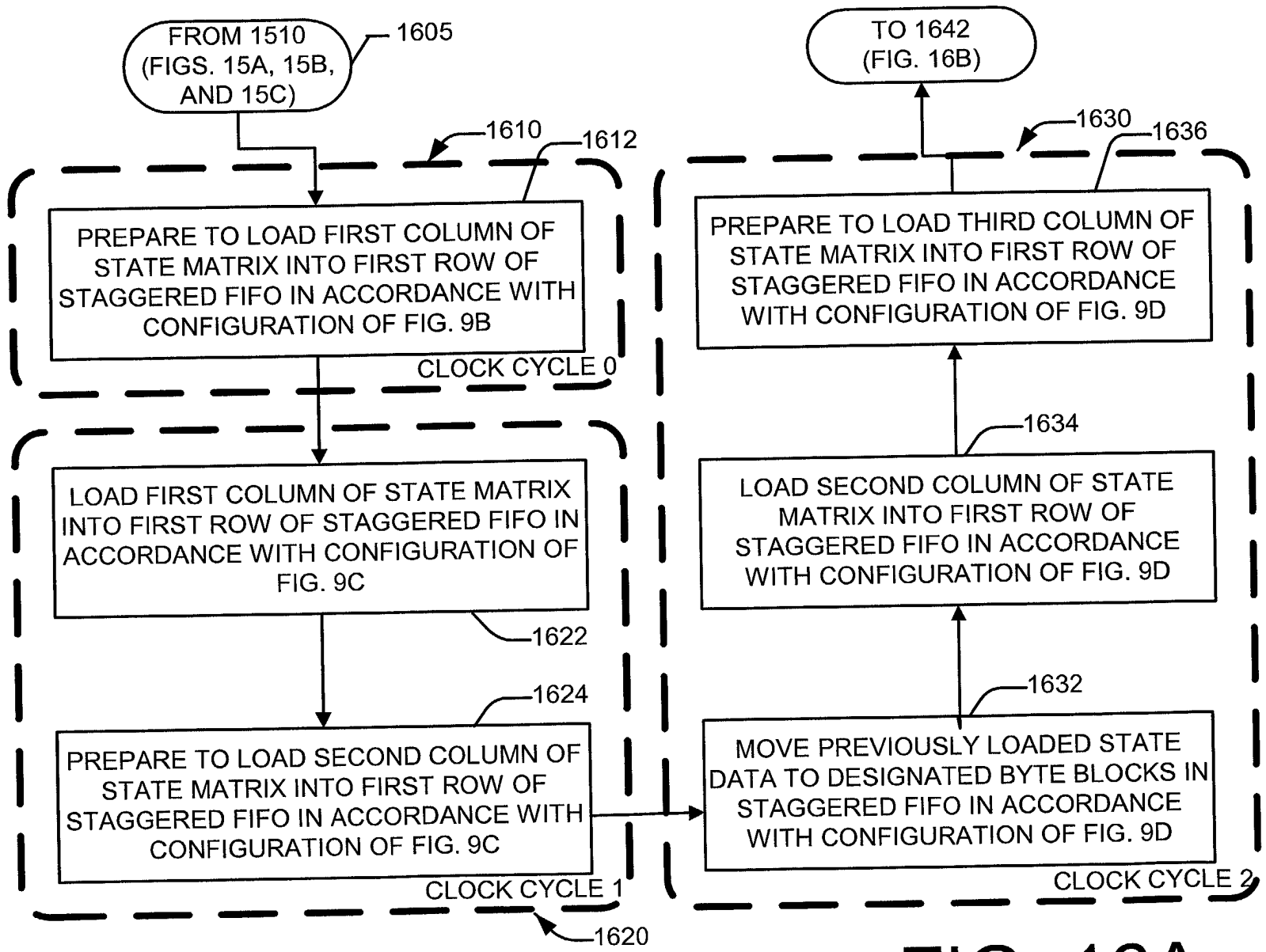

FROM 1510
(FIGS. 15A, 15B,
AND 15C)
1605
1610
1612
PREPARE TO LOAD FIRST COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9B
CLOCK CYCLE 0
LOAD FIRST COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9C
1622
1624
PREPARE TO LOAD SECOND COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9C
CLOCK CYCLE 1
1620
TO 1642
(FIG. 16B)
1630
1636
PREPARE TO LOAD THIRD COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9D
1634
LOAD SECOND COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9D
1632
MOVE PREVIOUSLY LOADED STATE DATA TO DESIGNATED BYTE BLOCKS IN STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9D
CLOCK CYCLE 2

FIG. 16A

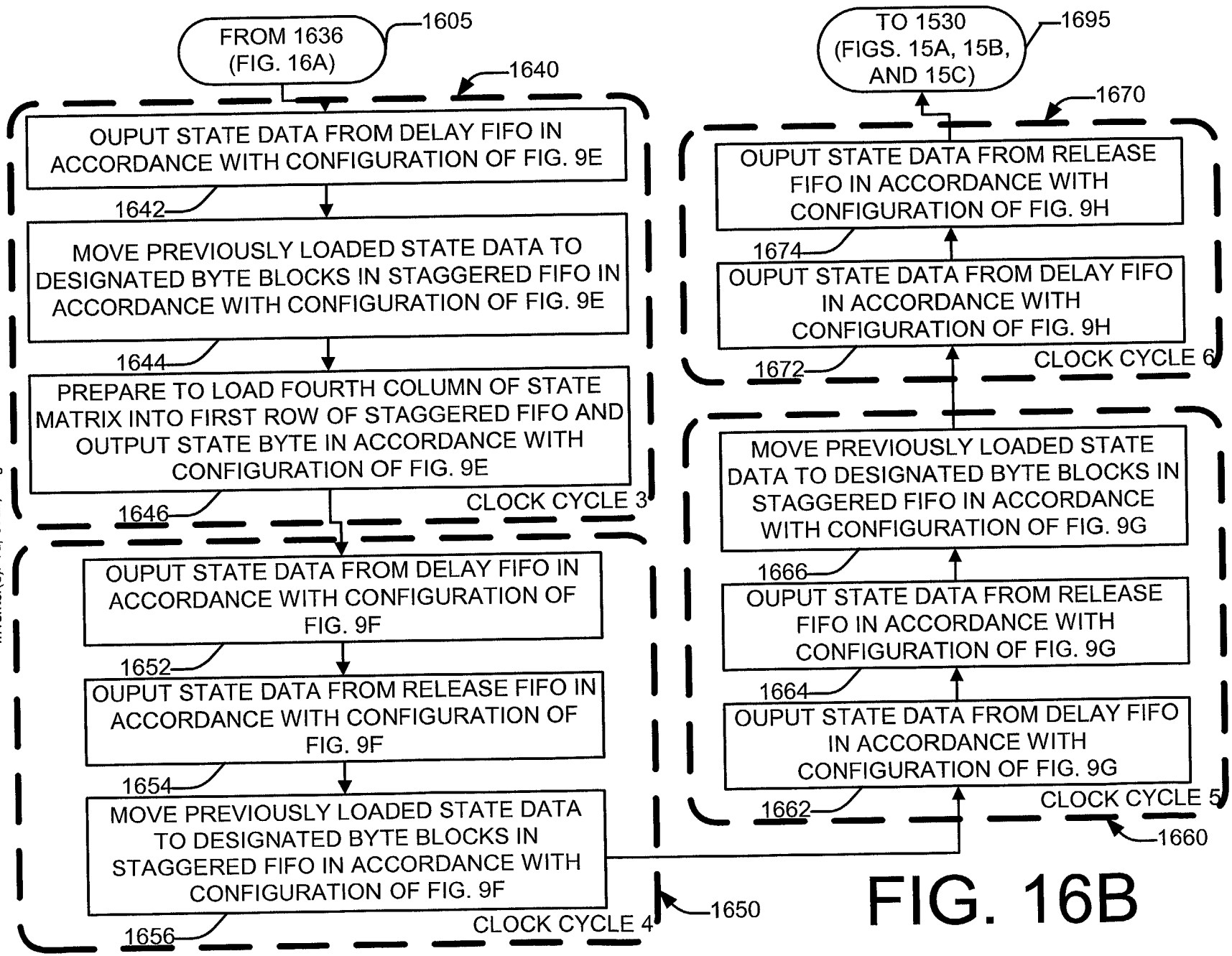

FROM 1636 (FIG. 16A)
1605
1640
OUPUT STATE DATA FROM DELAY FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9E
1642
MOVE PREVIOUSLY LOADED STATE DATA TO DESIGNATED BYTE BLOCKS IN STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9E
1644
PREPARE TO LOAD FOURTH COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO AND OUTPUT STATE BYTE IN ACCORDANCE WITH CONFIGURATION OF FIG. 9E
1646
CLOCK CYCLE 3
OUPUT STATE DATA FROM DELAY FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9F
1652
OUPUT STATE DATA FROM RELEASE FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9F
1654
MOVE PREVIOUSLY LOADED STATE DATA TO DESIGNATED BYTE BLOCKS IN STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9F
1656
CLOCK CYCLE 4
1650
MOVE PREVIOUSLY LOADED STATE DATA TO DESIGNATED BYTE BLOCKS IN STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9G
1666
OUPUT STATE DATA FROM RELEASE FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9G
1664
OUPUT STATE DATA FROM DELAY FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9G
1662
CLOCK CYCLE 5
1660
OUPUT STATE DATA FROM RELEASE FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9H
1674
OUPUT STATE DATA FROM DELAY FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9H
1672
CLOCK CYCLE 6
1670
TO 1530 (FIGS. 15A, 15B, AND 15C)
1695

FIG. 16B

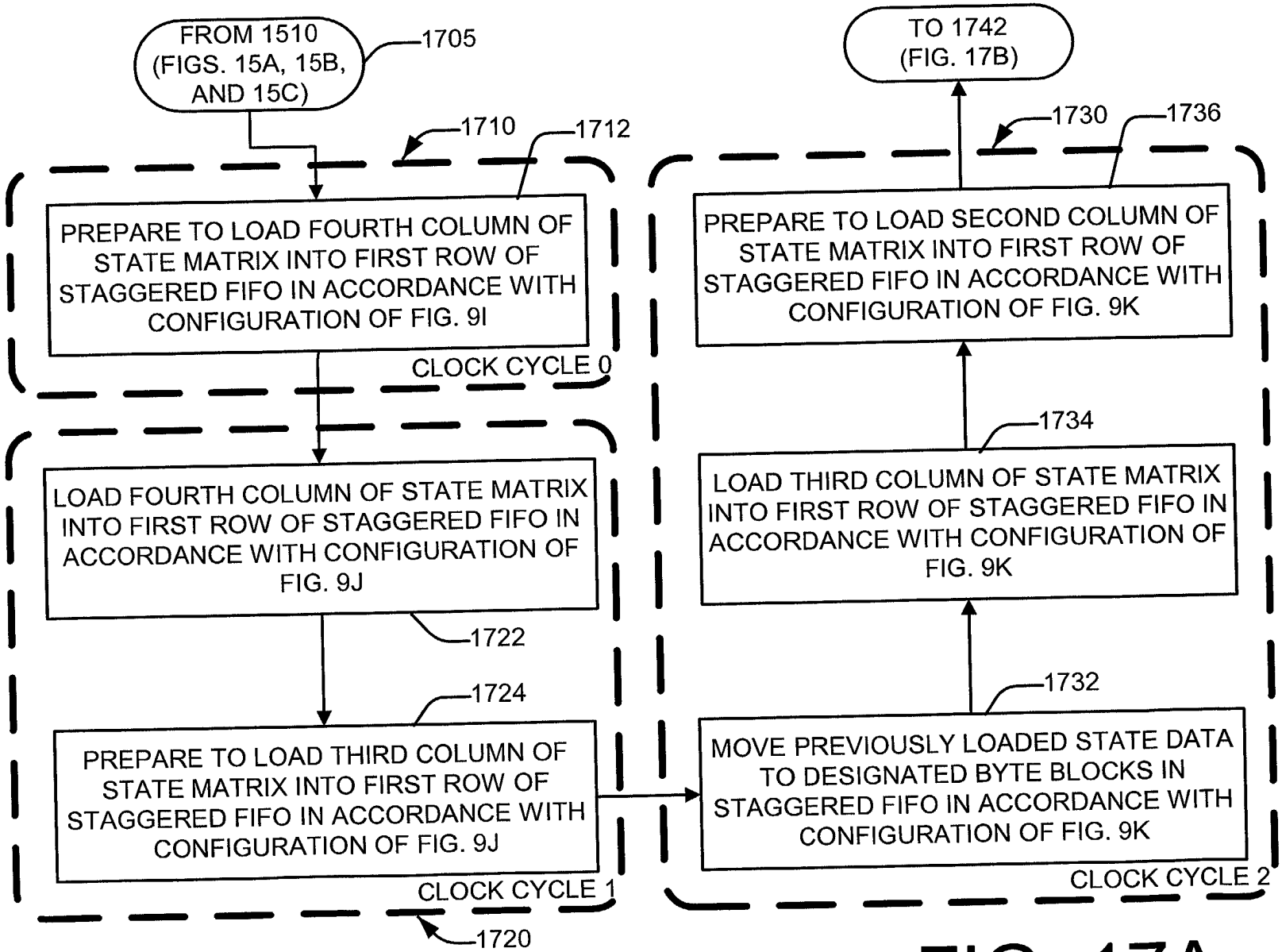

FROM 1510 (FIGS. 15A, 15B, AND 15C)
1705
1710
1712
PREPARE TO LOAD FOURTH COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9I
CLOCK CYCLE 0
LOAD FOURTH COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9J
1722
1724
PREPARE TO LOAD THIRD COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9J
CLOCK CYCLE 1
1720
TO 1742 (FIG. 17B)
1730
1736
PREPARE TO LOAD SECOND COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9K
1734
LOAD THIRD COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9K
1732
MOVE PREVIOUSLY LOADED STATE DATA TO DESIGNATED BYTE BLOCKS IN STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9K
CLOCK CYCLE 2

FIG. 17A

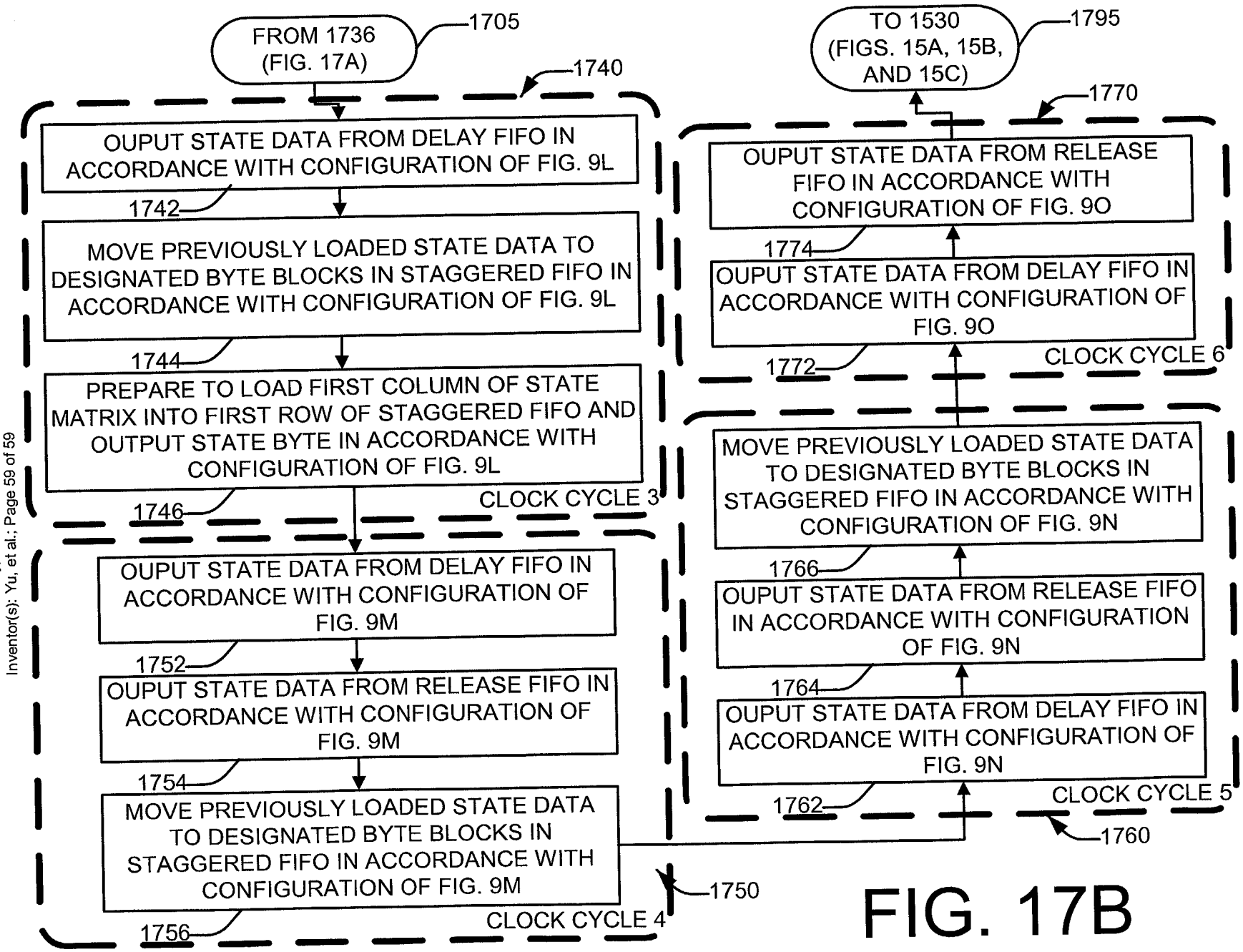

FROM 1736 (FIG. 17A)
1705
1740
OUPUT STATE DATA FROM DELAY FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9L
1742
MOVE PREVIOUSLY LOADED STATE DATA TO DESIGNATED BYTE BLOCKS IN STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9L
1744
PREPARE TO LOAD FIRST COLUMN OF STATE MATRIX INTO FIRST ROW OF STAGGERED FIFO AND OUTPUT STATE BYTE IN ACCORDANCE WITH CONFIGURATION OF FIG. 9L
1746
CLOCK CYCLE 3
OUPUT STATE DATA FROM DELAY FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9M
1752
OUPUT STATE DATA FROM RELEASE FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9M
1754
MOVE PREVIOUSLY LOADED STATE DATA TO DESIGNATED BYTE BLOCKS IN STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9M
1756
CLOCK CYCLE 4
1750
TO 1530 (FIGS. 15A, 15B, AND 15C)
1795
1770
OUPUT STATE DATA FROM RELEASE FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9O
1774
OUPUT STATE DATA FROM DELAY FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9O
1772
CLOCK CYCLE 6
MOVE PREVIOUSLY LOADED STATE DATA TO DESIGNATED BYTE BLOCKS IN STAGGERED FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9N
1766
OUPUT STATE DATA FROM RELEASE FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9N
1764
OUPUT STATE DATA FROM DELAY FIFO IN ACCORDANCE WITH CONFIGURATION OF FIG. 9N
1762
CLOCK CYCLE 5
1760

FIG. 17B